UNIVERSITY OF TRENTO

Faculty of Mathematical, Physical and Natural Sciences

Ph.D. Thesis

Computational problems in algebra: units in group rings and subalgebras of real simple Lie algebras

Advisor:
Prof. De Graaf Willem Adriaan

Candidate:
Faccin Paolo

Contents

1 Introduction

This thesis represents the work I did during my three years of Ph.D. studies. During my three years of my Ph.D. I worked on two unrelated topics, so I found very difficult to present my discoveries in a single organic paper. This is why I divided my thesis in two different blocks.

The first block is based on the research I did during the first year of my Ph.D. studies. During that time I approached the problem of finding generators for the unit group of an abelian group ring. This was a continuation of the research I did for my master thesis in mathematics. In that thesis my focus was to solve the problem of finding generators of the unit group of a different mathematical object: cyclotomic field $\mathbb{Q}(\zeta_n)$. There is a lot of literature regarding that subject and also a lot of constructions of finite index subgroups of the group of units. We studied and implemented in particular *Greither*'s construction [19]. Starting from his results we tried to find the whole group of units in the case of cyclotomic fields.
Once solved that problem, we focus on finding a way to obtain the group of units of abelian group algebras. The main reason is that, thanks to the *Wedderburn structure theorem*, every abelian group algebras over $\mathbb{Q}$ is isomorphic to a direct sum of cyclotomic fields, so we could use part of ours previous results and algorithms to solve this problem.
In a joint work with Willem De Graaf and Wilhelm Plesken we were able to produce and implement an algorithm for obtaining generators of the unit group of the integral group ring $\mathbb{Z}G$ of finite abelian group G. We use our implementation in MAGMA of this algorithm to compute the unit group of $\mathbb{Z}G$ for G of order up to 110. In particular for those cases we obtained the index of the group of Hoechsmann's units in the full unit group. Using the results we obtained we wrote an article, published in *Journal of Algebra* on October 2012, **"Computing generators of the unit group of an integral abelian group ring"**. [Faccin, De Graaf, Plesken].
I present our work during some conferences: MEGA on may 2011 (Stockholm) and *Advances in Group Theory and Applications* on June 2013 (Porto Cesareo Lecce (LE)).
Hoechsmann described in [22] a construction of a set of generators of a finite-index subgroup of $(\mathbb{Z}G)^*$, called the group of *constructible units*. Regarding this construction he wrote:

"Does this method ever yield all units if $n = |G|$ is not a prime power? The answer seem to be affirmative for $n < 74$".

In [22] this situation is not dealt with any further. Also, when $n = 74$ it is known that the group of constructible units is of index 3 in the full unit group (see [23]). So the question remains whether or not the constructible units generate the full unit group if $|G| < 74$. Using our implementation of our algorithms in the computer algebra system MAGMA [13] we have computed the unit groups for all abelian groups of order ≤ 110. We found 12 groups G of order less than 74 whose unit group is not generated by Hoechsmann units (namely, the groups of order 40, 48, 60, 63 and 65). It will be explained in more detailed later, but some of our results depends on the generalized Rienmann hypothesis.

The second block of my thesis is bases on the research I did during the second and third year of my Ph.D. studies. In the last two years I worked with Lie Algebras over $\mathbb{R}$.

The structure and representation theory of complex Lie algebras uses many combinatorial objects such as root systems, Weyl groups, weight lattices, Dynkin diagrams, etc., which makes the theory accessible for investigation by computer.
The finite dimensional real simple Lie algebras have been classified. However, it seems there has not been much effort to develop computer packages for investigating real semisimple Lie algebras by computer yet.
In my joint work with Heiko Dietrich and Willem De Graaf, *"Computing with real Lie algebras: real forms, Cartan decompositions, and Cartan subalgebras"*, we developed a computer algebra package, called `CoReLG` [53] ("*Computing with Real Lie Groups*"), for working with real semisimple Lie algebras given by a multiplication table.
Firstly it is shown how to construct multiplication tables of the real semisimple Lie algebras. Secondly, we show how to obtain a complete list of Cartan subalgebras or real simple Lie algebras $\mathfrak{g}$, that is a list containing exactly one elements of each G-conjugacy class of Cartan subalgebras of $\mathfrak{g}$, where G is the inner automorphism group of $\mathfrak{g}$. We describe algorithms for performing various tasks related to real simple Lie algebras. These algorithms form the basis of our software package `CoReLG`, written in the language of the computer algebra system GAP4.

After that I worked on problem of finding and classifying the semisimple subalgebras. This problem has previously been considered in the literature; Cornwell has published a series of papers on this topic, [50], [51], [67], [68], the last two in collaboration with Ekins. Their methods require detailed case-by-case calculations, and it is not entirely clear whether they are applicable to every subalgebra.
Komrakov [61] classified the maximal proper semisimple Lie subalgebras of a real simple Lie algebra. However, his paper does not give an account of the methods used. He also has a list of the real forms which contain a maximal S-subalgebra, for $\tilde{\mathfrak{g}}^c$ of exceptional type. We find the same inclusions as Komrakov, except that in type E_6 we find a few more (see Section 5.6).
Here we considered two problems. Let $\tilde{\mathfrak{g}}^c$ be a complex semisimple Lie algebra, and $\mathfrak{g}^c$ a complex semisimple subalgebra of $\mathfrak{g}^c$. Let then $\mathfrak{g} \subset \mathfrak{g}^c$ be a real form of $\mathfrak{g}^c$. The first question is **how to list, up to isomorphism, all real forms $\tilde{\mathfrak{g}} \subset \tilde{\mathfrak{g}}^c$ of $\tilde{\mathfrak{g}}^c$ such that $\mathfrak{g} \subset \tilde{\mathfrak{g}}$.**
The second problem that we considered is to find the regular semisimple subalgebras of a simple real Lie algebra. We give an algorithm to list the regular semisimple subalgebras of a semisimple real Lie algebra, up to conjugacy by the inner automorphism group. This uses the algorithm for listing the Cartan subalgebras of $\mathfrak{g}$, up to conjugacy. We have implemented this algorithm in the language of the computer algebra system GAP4. Using this implementation we have obtained the regular semisimple subalgebras of several real simple Lie algebras.

2 Group Algebras

In this chapter I show our results about the problem of finding generators of the unit group of an abelian group algebra over $\mathbb{Z}$.
In the next subsection I list some of the classical results that can be found in the literature about group algebras and I list some well known constructions of generating set of a finite-index subgroup of the unit group of $\mathbb{Z}G$.
In the second one I start by collecting some well-known facts and immediate observations concerning lattices, groups, associative algebras and one of the most important algorithms I use and implement, albeit not the original version; *Ge's algorithm* [4]. It is a very useful mathematical tool that allows to work easily with lattices and finding relations between units.
In the third one I describe our approach to computing the unit group of the maximal order in a cyclotomic field. This is a crucial step in our work, because, as I said before, thanks to Wedderburn's structure theorem all abelian group algebras over the rationals $\mathbb{Q}G$) are isomorphic to a direct sum of cyclotomic fields. There is strong a relationship between the units group $(\mathbb{Z}G)^*$ of an abelian group algebra and the unit group $\mathbb{Z}[\zeta_n]^*$ of a cyclotomic field: we have that the index $[\mathbb{Z}[\zeta_n]^* : (\mathbb{Z}G)^*]$ is finite and computable. But no theoretical estimate of this index is given.
The computation of the unit group is achieved by combining a construction by Greither [19] of a finite-index subgroup of the unit group, along with a MAGMA program by Fieker for *saturating* a subgroup at given prime p.
Subsection 4 contains the main algorithm of the paper we published, namely an algorithm for computing the unit group of an order $\mathcal{O}$ in a toral algebra A. The main idea is to split A into its simple ideals e_iA where the e_i are the orthogonal primitive idempotents. The e_iA are number fields with orders $e_i\mathcal{O}$. So in order to compute their unit group we can use the effective version of the Dirichlet unit theorem (cf. [2], [26]). The basic step of the algorithm is, given two orthogonal idempotents e_1, e_2, to obtain the unit group of $(e_1 + e_2)\mathcal{O}$ given the unit group of $e_i\mathcal{O}$, $i = 1, 2$.
In subsection 5 I describe our method for obtaining generators of unit groups of integral abelian group rings. Its main ingredients are: the construction of the unit groups of cyclotomic fields, and the algorithm of section 4. I also give some comments on the Runtimes of the implementation of the algorithm in MAGMA, and we give a table containing all abelian groups of order up to 110, where the constructible (or *Hoechsmann*'s) units do not generate the full unit group. For all the groups we find other units (the so called *exotic units*) I give the index of the group of constructible units in the full unit group.

In the main algorithms and implementations we make essential use of Fieker's implementation in MAGMA of an algorithm by Ge [4] to obtain a basis of a lattices

$$\{(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n \mid u_1^{\alpha_1} \ldots u_n^{\alpha_n} = 1\}$$

of the multiplicative relations of given elements $u_1, \ldots, u_n$ in a number field.

2.1 Classical result about unit group of group algebras

Definition 1. Let G be a finite abelian group. For a ring R we let RG be the group ring over R, consisting of sums of the form $\sum_{g\in G} a_g g$, with $a_g \in R$. We take $R = \mathbb{Z}$ and consider the unit groups:

$$(\mathbb{Z}G)^* = \{u \in \mathbb{Z}G \mid \text{ there is a } v \in \mathbb{Z}G \text{ with } vu = 1\}.$$

Many mathematicians worked on the problem of finding structure properties of this group, such as decomposition or rank. Once solved this problem, the next step was to find a group of generators of it, or at least to find generators for a finite-index subgroup of $(\mathbb{Z}G)^*$. Here I list some of the classical results that can be found in the literature.
In the 40's Graham Higman [21] showed that:

Proposition 1. $(\mathbb{Z}G)^* = \pm G \times F$, where F is a free abelian group.

But he didn't give any bound on its rank. This problem was solved thanks to Ayoub and Ayoub [10] on 1969; they showed that:

Proposition 2.

$$rk(F) := \frac{1}{2}(|G| + 1 + t_2 - 2l)$$

where t_2 is the number of elements of G of order 2, and l is the number of cyclic subgroups of G.

Various construction of finite index subgroups of $(\mathbb{Z}G)^*$ have appeared in the literature (see [27]). Among these I present two of them. the first one is due to Bass, who construct a subgroup using what he called **Bass cyclic units**. The other one is due to Hoechsmann, his construction is a refinement of the one made by Bass and seems to yield subgroups of particular small index. To show the differences between Hoechsmann's construction and Bass's construction we have computed the index of the group of Bass cyclic units in the group of Hoechsmann units, for some group G.

2.1.1 Bass construction

Here we describe Bass construction of a finite-index subgroup of the unit group $(\mathbb{Z}G)^*$.

Definition 2. Let G be a finite group, and g be an element of G of order n. Set $\widehat{g} = \sum_{k=0}^{n-1} g^k$. A **Bass cyclic unit** is an element of the group ring $\mathbb{Z}G$ of the form:

$$\mu_i := (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\widehat{g}$$

where i is an integer such that $1 < i < n - 1$ and $\gcd(i, n) = 1$.

The Bass cyclic units are, in fact, invertible, with inverse:

$$\mu_i^{-1} := (1 + g^i + \cdots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\widehat{g}$$

where k is any integer such that $ik \equiv 1 \mod n$. These units are of infinite order in $(\mathbb{Z}G)^*$. Furthermore, we have the following:

Theorem 1. Let G be a finite abelian group. Then $\mathcal{B}$, the group generated by all Bass cyclic units of $\mathbb{Z}G$, is of finite index in $(\mathbb{Z}G)^*$.

2.1.2 The group of Hoechsmann unit $\mathcal{H}$

Here we briefly describe Hoechsmann's construction [22] of a finite-index subgroup of the unit group $(\mathbb{Z}G)^*$.

Definition 3. Let C be a cyclic group of order n, generated by the element x. For $i \geq 0$ and $y \in C$ we set

$$s_i(y) = 1 + y + \cdots + y^{i-1}.$$

Let i, j be integers with $0 < i, j < n$ and $\gcd(i, n) = \gcd(j, n) = 1$. Let k, l be positive integers with $li = 1 + kn$. Set

$$u_{i,j}(x) = s_l(x^i)s_i(x^j) - ks_n(x).$$

Then $u_{i,j}(x)$ is a unit in $(\mathbb{Z}C)^*$. Let $\Theta(C)$ denote the set of all units constructed in this way. We let $\mathcal{H}$ be the group of units in $(\mathbb{Z}G)^*$ generated by all $\Theta(C)$, where C ranges over the cyclic subgroups of G of order > 2, along with $\pm G$. It is called the group of **constructible units** of $\mathbb{Z}G$.

Theorem 2. $\mathcal{H}$ is a subgroup of finite index of $(\mathbb{Z}G)^*$. If this index is not one, the independent units not belonging to $\mathcal{H}$ are called **exotic units** of $\mathbb{Z}G$.

In general the set consisting of the $u_{i,j}(x)$ is a heavily redundant generating set. However, from [23] we have the following theorem.

Theorem 3. Let m be the exponent of G, and set $H_m = (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$. Suppose that H_m is a cyclic group, and let $i \in \mathbb{Z}$ induce a generator of H_m. Then $\mathcal{H}$ is generated by $\pm G$ along with $u_{i,i}(z)$, where z runs through G.

This gives a much more efficient way of constructing $\mathcal{H}$. We remark that H_m is cyclic with only few exceptions. The values of m up to 120, for which H_m is not cyclic, are 24, 40, 48, 56, 60, 63, 65, 72, 80, 84, 85, 88, 91, 96, 104, 105, 112, 117, 120.

Although the group $\mathcal{B}$ is of finite index in the group $(\mathbb{Z}G)^*$, it is not a good approximation of it. We computed the index $[\mathcal{H} : \mathcal{B}]$ for some small groups and listed the results in the next table. From the literature it is known that $\mathcal{H}$ is bigger than $\mathcal{B}$, but this table give us an insight of how much $\mathcal{H}$ is an improvement of $\mathcal{B}$ even for small values of n. We note that, if $|G|$ is a prime number, the index $[\mathcal{H} : \mathcal{B}]$ tends to be large and grows up very quickly. Moreover, the gain of using $\mathcal{H}$ instead of $\mathcal{B}$ also increases with the growth of the rank of the group $(\mathbb{Z}G)^*$.
Hoechsmann was very confident of his method; regarding this construction he wrote:

"Does this method ever yield all units if $n = |G|$ is not a prime power? The answer seem to be affirmative for $n < 74$".

In [22] this situation is not dealt with any further. Also, when $n = 74$ it is known that the group of constructible units is of index 3 in the full unit group (see [23]). So the question remains whether the constructible units generate the full unit group if $|G| < 74$. Using our implementation of our algorithms in the computer algebra system MAGMA [13] we have computed the unit groups for all abelian groups of order ≤ 110. We found 12 groups G of order less than 74 whose unit group is not generated by Hoechsmann units (namely, the groups of order 40, 48, 60, 63 and 65).

Group G	**Index** $[\mathcal{H} : \mathcal{B}]$	**Rank of** $(\mathbb{Z}G)^*$
C_{10}	4	2
C_{11}	2000	4
C_{12}	2	1
$C_2 \times C_6$	1	0
C_{17}	33554432	7
C_{18}	144	4
$C_3 \times C_6$	1	0
C_{19}	1224440064	8
C_{24}	512	5
$C_2 \times C_{12}$	4	2
$C_2 \times C_2 \times C_6$	1	0
C_{27}	14693280768	10
$C_3 \times C_9$	1728	6
$C_3 \times C_3 \times C_3$	1	0
C_{30}	65536	8
C_{31}	31886460000000000000	14

Table 1: Index $[\mathcal{H} : \mathcal{B}]$ for some group G

2.2 Lattices

In this section I will outline some algorithm to compute a basis for a lattice and for computing the intersection of lattices.

Definition 4. A *lattice* in $\mathbb{Z}^m$ is a finite generated subgroup of it. A lattice $\Lambda \subset \mathbb{Z}^m$ has a basis, that is a subset $u_1, \ldots, u_r$ such that every $u \in \Lambda$ can uniquely be written as $u = \sum_{i=1,r} \alpha_i u_i$, with $\alpha_i \in \mathbb{Z}$. The lattice $\Lambda \subset \mathbb{Z}^m$ is called pure if $\mathbb{Z}^m/\Lambda$ is torsion-free (See [14], §III.16.)

Let $\Lambda \subset \mathbb{Z}^m$ be a lattice with basis $u_1, \ldots, u_r$. we form the $r \times m$-matrix B with rows consisting of the coefficients of the u_i with respect to the standard basis of $\mathbb{Z}^m$. By computing the Smith normal form of B we can effectively compute the homorphism $\Psi : \mathbb{Z}^m \to \mathbb{Z}^m/\Lambda$ [ref]. Let T denote the torsion submodule of $\mathbb{Z}^m/\Lambda$. Then $\Psi^{-1}(T)$ is the smallest pure lattice containing Λ So in particular, the Smith normal form algorithm gives a method to compute a basis of the lattice $V \cap \mathbb{Z}^m$ where V is a subspace of $\mathbb{Q}^m$. For example, we can compute the intersection of lattices in this way.
As shown in (See [14], §III.16.), a lattice is pure if and only if it is a direct summand of $\mathbb{Z}^m$. So in that case, by computing the Smith normal form, we can compute a basis of $\mathbb{Z}^m$ such that the first r basis elements for a basis of Λ.

2.2.1 Ge's algorithm

We now describe Ge's algorithm for computing multiplicative relations among algebraic integers. It has been published in his thesis. This is a very important algorithm for our purposes because it allows us, not only to compute multiplicative relations between units, but also to find a basis for a lattice and even to easily computing the index of two subgroups.

Let $K \supset \mathbb{Q}$ be a number field, and $\varepsilon_1, \ldots, \varepsilon_s$ algebraic integers in K. The problem is to find a basis of the lattice:

$$\Lambda = \{(e_1, \ldots, e_s) \in \mathbb{Z}^s \mid \prod_{i=1}^{s} \varepsilon_i^{e_i} = 1\}.$$

In [4], Guoqiang Ge developed an attractive algorithm for this. Here we describe his algorithm. Combining it with a bound due to Masser [6], leads to a, more efficient version of the algorithm. We divide this section into two subsections.
At first we present an algorithm for finding a basis of what we call the perp-lattice of a lattice. As its main step it uses the LLL lattice basis reduction algorithm. After that, we consider the original problem, i.e. computing multiplicative relations among algebraic integers. It is shown that it can be solved by computing a basis of the perp-lattice of a certain lattice.

2.2.2 Finding a basis of the perp-lattice

Definition 5. A lattice in $\mathbb{R}^n$ is a subset of it of the form:

$$\{\sum_{i=1}^{s} \alpha_i v_i \mid \alpha_i \in \mathbb{Z}\}$$

where $v_1, \ldots, u_n \in R^n$ are linearly independent.

It can be shown that $L \in \mathbb{R}^n$ is a lattice if and only if it is a subgroup and there is a $\lambda > 0$ such that $\|\|v\|\| > \lambda$ for all $v \in L$.

Let $v_1, \ldots, v_s \in \mathbb{R}^n$ be given. Set:

$$L := \{\textstyle\sum_{i=1}^{s} \alpha_i v_i \mid \alpha_i \in \mathbb{Z}\} \text{ and } \Lambda_0 := \{(e_1, \ldots, e_s) \in \mathbb{Z}^s \mid \textstyle\sum_{i=1}^{s} e_i v_i = 0\}.$$

Then $\Lambda_0 \subset \mathbb{Z}^s$ is also a lattice over $\mathbb{Z}$. We call it the perp-lattice of L. We suppose that:

- L is a lattice in $\mathbb{R}^n$, and
- a $\lambda > 0$ is given with $\|v\| > \lambda$ for all nonzero $v \in L$.
- we have approximations of the v_i, i.e., $w_i \in \mathbb{R}^n$ with $10^t w_i \in \mathbb{Z}^n$ and $|w_{i_j} - v_{i_j}| \leq 10^{-t}$ (where by w_{i_j} we denote the j-th coordinate of w_i).
- we are given an $M > 0$ such that Λ_0 has a basis consisting of elements u with $\|u\| \leq M$.

Below we will describe how t should be chosen. The problem considered in this section is to find a basis of Λ_0. Throughout ℓ will denote the rank of Λ_0 (which we do not assume to be known). For $1 \leq i \leq s$ let $b_i = (f_i \mid 10^t w_i) \in \mathbb{Z}^{n+s}$, where $f_i \in \mathbb{Z}^n$ has a 1 on position i, and all other coordinates equal to 0. So the matrix with rows $b_1, \ldots, b_s$ is obtained by appending to the identity matrix the matrix with rows $10^t w_i$. Let L_t be the lattice spanned by $b_1, \ldots, b_s$. For $e = (e_1, \ldots, e_s) \in \mathbb{Z}^s$ we set $\hat{e} = \sum_{i=1}^{s} e_i b_i$. Then a straightforward calculation shows that:

$$\|\hat{e}\|^2 = \|e\|^2 + 10^{2t} \|\textstyle\sum_{i=1}^{s} e_i w_i\|^2.$$

We set $\varepsilon_i = w_i - v_i$. Then $\|\varepsilon_i\|^2 \leq 10^{-2t} n$.

Proposition 3. Let $u \in \Lambda_0$ be such that $\|u\| \leq M$. Then $\|\hat{u}\| \leq \sqrt{1+sn}M$.

Proof. Write $u = (u_1, \ldots, u_s)$. Observe that $\sum_j u_j w_j = \sum_j u_j \varepsilon_j$. Using this, and the Cauchy-Schwarz inequality we get:

$$\|\hat{u}\|^2 = \|u\|^2 + 10^{2t}\|\sum_{j=1}^{s} u_j\varepsilon_j\|^2 \leq \|u\|^2 + 10^{2t}\|u\|^2 \sum_{j=1}^{s}\|\varepsilon_j\|^2 \leq M^2(1+ns).$$

□

Proposition 4. Let $U > 0$, and choose t such that $10^t \geq U(\sqrt{sn}+1)/\lambda$. Let $u \in \mathbb{Z}^s$ be such that $u \notin \Lambda_0$. Then $\|\hat{u}\| > U$.

Proof. If $\|u\| \geq U$ then this is clear; so suppose $\|u\| < U$. Let us write $u = (u_1, \ldots, u_s)$. Then:

$$\begin{aligned}
\|\hat{u}\| > 10^t\|\sum_{i=1}^{s} u_i w_i\| = 10^t\|\sum_{i=1}^{s} u_i v_i + \sum_{i=1}^{s} u_i\varepsilon_i\| &\geq 10^t\left(\|\sum_{i=1}^{s} u_i v_i\| - \|\sum_{i=1}^{s} u_i\varepsilon_i\|\right) \\
&\geq 10^t\left(\lambda - \sum_{i=1}^{s}|u_i|\|\varepsilon_i\|\right) \geq 10^t\left(\lambda - \sqrt{\sum_{i=1}^{s} u_i^2}\sqrt{\sum_{i=1}^{s}\|\varepsilon_i\|^2}\right) \\
&\geq 10^t(\lambda - U\sqrt{sn}10^{-t}) \geq U.
\end{aligned}$$

□

Next we need the celebrated LLL-algorithm. The next theorem is [5], Proposition 1.12 (and also [2], Theorem 2.6.2(5)).

Theorem 4. Let $\Lambda \subseteq \mathbb{Z}^r$ be a lattice. Suppose that Λ contains linearly independent elements $x_1, \ldots, x_l$ of norm $\|x_i\| \leq D$. Then for an LLL-reduced basis $b_1, \ldots, b_k$ of Λ we have:

$$\|b_i\|^2 \leq 2^{r-1}D^2 \text{ for } 1 \leq i \leq l.$$

Now we have all ingredients for the algorithm for finding a basis of Λ_0, which runs as follows.

1. Set $U = 2^{\frac{s+n}{2}}\sqrt{1+sn}M$, and choose t such that $10^t \geq U(\sqrt{sn}+1)/\lambda$.
2. Let $\hat{b}_1, \ldots, \hat{b}_s$ be an LLL-reduced basis of L_t.
3. Let ℓ_0 be such that $\|\hat{b}_i\| \leq U$ for $1 \leq i \leq \ell$, and $\|\hat{b}_i\| > U$ for $i > \ell_0$.
4. Then Λ_0 is spanned by $b_1, \ldots, b_{\ell_0}$ and $\ell = \ell_0$.

Remark 2.1. Note that by Proposition 3, L_t contains ℓ linearly independent elements $\hat{u}_i$ with $\|\hat{u}_i\| \leq \sqrt{1+sn}M$. Therefore, by Theorem 4, $\|\hat{b}_i\| \leq U$ for $1 \leq i \leq \ell$. By Proposition 4 the b_i lie in Λ_0 for $i \leq \ell$. Observe that $b_1, \ldots, b_s$ form a basis of $\mathbb{Z}^s$. So an $u \in \Lambda_0$ can be written $u = \sum_{i=1}^{s} \alpha_i b_i$, with $\alpha_i \in \mathbb{Z}$. If $v = \sum_{i=\ell+1}^{s} \alpha_i b_i$ is nonzero, then Λ_0 contains $\ell + 1$ linearly independent vectors (i.e., $b_1, \ldots, b_\ell, v$). But that is impossible. It follows that $b_1, \ldots, b_\ell$ are a basis of Λ_0. For the last statement note that by Proposition 4, $b_1, \ldots, b_{\ell_0}$ lie in Λ_0. Hence $\ell_0 \leq \ell$. But since $\|\hat{b}_i\| \leq U$ for $1 \leq i \leq \ell$ it follows that $\ell_0 \geq \ell$.

2.2.3 The lattice

In this subsection we show how we can use the algorithm of the previous subsection to get a basis of the lattice Λ.
For a $z = re^{i\theta} \in \mathbb{C}$ we have $\log(z) = \log(r) + i\theta$, where we take $\theta \in [0, 2\pi)$. This means that $\log(z_1 z_2) = \log(z_1) + \log(z_2) \bmod 2\pi i$. For $z \in \mathbb{C}$ we denote its norm by $|z|$. Let $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ be all embeddings of K into $\mathbb{C}$.
For a $z \in \mathbb{C}$ we write $|z + i\mathbb{Z}| = \min_{m \in \mathbb{Z}} |z + im|$.

Proposition 5. Let $0 \neq \varepsilon \in K$ be an algebraic integer. If $|\frac{1}{2\pi}\log(\sigma_j(\varepsilon)) + i\mathbb{Z}| \leq \frac{1}{10}$ for $i \leq j \leq n$, then $\varepsilon = 1$.

Proof. Let $z \in \mathbb{C}$ with $|z| \leq \frac{1}{10}$. Then:

$$|e^{2\pi z} - 1| = |\sum_{k=1}^{\infty} \frac{(2\pi z)^k}{k!}| \leq \sum_{k=1}^{\infty} \frac{|2\pi z|^k}{k!} = e^{|2\pi z|} - 1 \leq e^{\frac{2\pi}{10}} - 1 < 1.$$

For $1 \leq j \leq n$ there is $a_j \in \mathbb{Z}$ with $|\frac{1}{2\pi}\log(\sigma_j(\varepsilon)) + ia_j| \leq \frac{1}{10}$. Hence:

$$|\sigma_j(\varepsilon) - 1| = |e^{2\pi \frac{1}{2\pi}\log(\sigma_j(\varepsilon))} - 1| = |e^{2\pi(\frac{1}{2\pi}\log(\sigma_j(\varepsilon)) + a_j i)} - 1| < 1.$$

Therefore $|N(\varepsilon - 1)| = \prod_j |\sigma_j(\varepsilon) - 1| < 1$. But, since $\varepsilon - 1$ is an algebraic integer, the norm of $\varepsilon - 1$ is an integer. Hence its norm is 0, and $\varepsilon = 1$.

□

Now we define $\sigma : K \to \mathbb{R}^{2n}$ by:

$$\sigma(a) = \tfrac{1}{2\pi}(\Re(\log(\sigma_1(a))), \Im(\log(\sigma_1(a))), \ldots, \Re(\log(\sigma_n(a))), \Im(\log(\sigma_n(a)))).$$

For $1 \leq j \leq n$ let v_j be the element of $\mathbb{R}^{2n}$ with a 1 on position $2j$, and zeros elsewhere. Let $V \subset \mathbb{R}^{2n}$ be the space spanned by the vectors v_j. Then we have that $\sigma(ab) = \sigma(a) + \sigma(b) \bmod V$. Let $\varepsilon_1, \ldots, \varepsilon_s \in K$ be algebraic integers, and set $u_j = \sigma(\varepsilon_i)$. Let $L \subset \mathbb{R}^{2n}$ be the $\mathbb{Z}$-module generated by $u_1, \ldots, u_s, v_1, \ldots, v_n$.

Proposition 6. Let $w \in L$ be nonzero. Then $\|w\| \geq \frac{1}{10}$. In particular, L is a lattice in $\mathbb{R}^{2n}$.

Proof. We have $w = \sum_j \alpha_j u_j + \sum_k \beta_k v_k$, where $\alpha_j, \beta_k \in \mathbb{Z}$. Set $\varepsilon = \prod_{j=1}^{s} \varepsilon_j^{\alpha_j}$. Then $\sigma(\varepsilon) = \sum_j \alpha_j u_j \bmod V$. If $\varepsilon \neq 1$, then it follows that

$$\|w\| \geq \max_{1 \leq j \leq n} |\tfrac{1}{2\pi}\log(\sigma_j(\varepsilon)) + \mathbb{Z}i| \geq \frac{1}{10},$$

by Proposition 5. On the other hand, if $\varepsilon = 1$, then the odd coordinates of w are zero, whereas the even coordinates are integers. Hence $\|w\| \geq 1$.

□

Now set: $\Lambda_0 = \{(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_n) \in \mathbb{Z}^{s+n} \mid \sum_{j=1}^{s} \alpha_j u_j + \sum_{k=1}^{n} \beta_k v_k = 0\}$, i.e., Λ_0 is the perp-lattice of L. Next we show that Λ_0 has a basis consisting of vectors whose norm is bounded by an explicitly given constant. For this we use a bound due to Masser [6], as well as the discussion in [3].
We need the logarithmic height $h : K \to \mathbb{R}$, which is defined as follows.

Definition 6. For $\alpha \in K$ we let $f \in \mathbb{Z}[x]$ be its minimal polynomial, with positive leading coefficient. We write $f = a(x - \alpha_1) \cdots (x - \alpha_d)$ and set:

$$M(\alpha) = a \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

Then:

$$h(\alpha) \doteq \log(M(\alpha))/d.$$

We let h_0 be the maximum of the $h(\varepsilon_i)$, if that maximum is positive. Otherwise we set $h_0 = \log(2)$ and we note that $n = [K : \mathbb{Q}]$. If $n \geq 3$ we set:

$$\eta_0 = \tfrac{1}{4n} \left(\tfrac{\log\log n}{\log n} \right)^3,$$

and $\eta_0 = \log(1.17)/2$ if $n = 2$. Furthermore: $R = s^{s-1}(n+1)^2 \left(\frac{h_0}{\eta_0} \right)^{s-1}$.
As before set $\Lambda = \{(e_1, \ldots, e_s) \in \mathbb{Z}^s \mid \prod_{j=1}^{s} \varepsilon_j^{e_j} = 1\}$.

Lemma 1. Λ has a basis consisting of elements $\underline{e} = (e_1, \ldots, e_s)$ with $|e_i| \leq R$.

Proof. In [6] it is shown that Λ has a basis consisting of the vectors $\overline{e}$ with $|e_i| \leq s^{s-1}\omega(h/\eta)^{s-1}$. Here η is the infimum of $h(\alpha)$ with $\alpha \in K$ not a root of unity. It was shown by Voutier [9] that $h(\alpha) > \eta_0$ if $n \geq 3$. But for $n = 2$ it is known that $M(\alpha) > 1.17$ (cf. [1]). Next, h is the maximum of the $h(\varepsilon_i)$ and η. Since the height of 2 is $\log(2)$, we get $h \leq h_0$. Finally, ω is the maximal order of a root of unity in K. This means that $\varphi(\omega) \leq n$, where φ is the Euler function. But $\varphi(\omega) > \sqrt{\omega} - 1$. □

Define $\phi : \Lambda_0 \to \Lambda$ by $\phi(\alpha_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_s)$. Then the map ϕ is bijective; so computing a basis of Λ_0 solves the problem.

Proposition 7. Λ_0 has a basis consisting of elements of norm bounded by $M = R\sqrt{s(1+ns)}$.

Proof. Consider an embedding $\sigma_k : K \to \mathbb{C}$, and write:

$$\log(\sigma_k(\varepsilon_j)) = \log(r_{k,j}) + i\theta_{k,j}, \text{ with } 0 \leq \theta_{k,j} < 2\pi.$$

Let $\underline{e} = (e_1, \ldots, e_s) \in \Lambda$, be such that it satisfies $|e_j| \leq R$. Taking the logarithm of $\varepsilon_1^{e_1} \cdots \varepsilon_s^{e_s} = 1$ we obtain:

$$\sum_{j=1}^{s} e_j \log(\sigma_k(\varepsilon_j)) = i \sum_{j=1}^{s} e_j \theta_{k,j}$$

The last sum is equal to $r \cdot 2\pi$ with $|r| \leq \sum_{j=1}^{s} |e_j| \leq sR$. Hence under ϕ, we have that $\underline{e}$ corresponds to $(e_1, \ldots, e_s, \beta_1, \ldots, \beta_n) \in \Lambda_0$ with $|\beta_i| \leq sR$. Combining this with Lemma 1 we get the statement of the proposition.

□

Now we have all data necessary to apply the algorithm of Section 2.2.2 to the lattice L. Indeed, $\lambda = \frac{1}{10}$ and $M = R\sqrt{s(1+ns)}$. In order to apply the algorithm of Section 2.2.2 we need to compute $\log(\sigma_i(\varepsilon_j))$ to a given precision.
There are algorithms for computing the complex roots of a polynomial to a given precision (for example Schönhage's algorithm, [8]). Using this for the minimal polynomial of a primitive element of K, we approximately find the embeddings σ_i. Also there are algorithms to compute approximations for the logarithm (cf. [7]). Ge's thesis contains a result stating the precision to which the roots of the minimum polynomial of a primitive element have to be computed in order to reach a given precision of $\log(\sigma_i(\varepsilon_j))$. Here we do not go into this.
Also, in order to compute the number R we need to compute approximations for the heights of the ε_j. For this we use the definition, along with the algorithm for computing approximations of the roots of a polynomial.

Remark 2.2. Instead of the bound M, Ge derived a bound using an upper bound on the norm of the vectors v_i (notation as in Section 2.2.2). This yields a bound that depends on the degree of K, n, like $(2n)^{2n}$.
The bound that is used is much more sensitive to the number of algebraic integers ε_i. As in our application this number is usually rather low, whereas the degree can grow arbitrarily, this works better for our purposes.

Example.
Let K be the field $\mathbb{Q}(\sqrt{2})$ and $\varepsilon_1 = 12\sqrt{2}+17$, $\varepsilon_2 = -1$, $\varepsilon_3 = -408\sqrt{2}+577$. Note that all of them are a units in $\mathbb{Q}(\sqrt{2})$. We want to find a basis of the lattice Λ consisting of all $(e_1, e_2, e_3) \in \mathbb{Z}^3$ with $\varepsilon_1^{e_1}\varepsilon_2^{e_2}\varepsilon_3^{e_3} = 1$.
Using MAGMA we compute approximations:

$$h(\varepsilon_1) = 1.76,\ h(\varepsilon_2) = 0,\ h(\varepsilon_3) = 3.525.$$

Hence we can take $h_0 = 3.6$. Also, $\eta_0 = \log(1.17)/2 > 0.078$. With this we get that $M = 790697.68$ (cf. Proposition 7). In the notation of Section 2.2.2, using M as above, $n = 4$, $s = 5$ and $\lambda = \frac{1}{10}$, we get:

$$U = 81988905.7, \text{ and } U(\sqrt{sn}+1)/\lambda = 4486544391.0.$$

So we can use $t = 10$. Using approximations of $\log(\varepsilon_i)$ we get that L_{10} is spanned by the rows of the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 5610998523 & 0 & -5610998523 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 5\cdot 10^9 & 0 & 5\cdot 10^9 \\ 0 & 0 & 1 & 0 & 0 & -11221997046 & 0 & 11221997046 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 10^{10} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 10^{10} \end{pmatrix}.$$

An LLL-reduced basis of L_{10} is given by the rows of the following matrix:

$$\begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 5610998523 & 0 & -5610998523 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 5\cdot 10^9 & 0 & 5\cdot 10^9 \\ 0 & -1 & 0 & 1 & 0 & 0 & 5\cdot 10^9 & 0 & -5\cdot 10^9 \end{pmatrix}.$$

Hence Λ is spanned by $(2,0,1)$ and $(0,-2,0)$.

2.2.4 Pure Lattices

A lattice $\Lambda \subset \mathbb{Z}^m$ has a basis, that is a subset $u_1, \cdots, u_r$ such that every $u \in \Lambda$ can uniquely be written as $u = \sum_{i=1}^{r} \alpha_i u_i$, with $\alpha_i \in \mathbb{Z}$. The integer r is called the rank of Λ. Let $\Lambda \subset \mathbb{Z}^m$ be a lattice with basis $u_1, \cdots, u_r$. We form the $r \times m$-matrix B with rows consisting of the coefficients of the u_i with respect to the standard basis of $\mathbb{Z}^m$. There are algorithms to compute the Smith normal form of B (cf. [27]), that is, integral matrices S, P, Q with the following properties:

- P and Q are, respectively, $r \times r$ and $m \times m$ unimodular matrices.
- S is an $r \times m$-matrix with zeros outside the diagonal, and the $d_i = S(i,i)$ satisfy $d_i | d_{i+1}$.
- $S = PBQ$.

We note that this implies that the rows $q_1, \cdots, q_m$ of Q^{-1} are a basis of $\mathbb{Z}^m$ such that $d_i q_i \in \Lambda$ for $1 \leq i \leq r$.

Definition 7. We say that a lattice $\mathbb{Z}^m$ is pure if for all $u \in \Lambda$ and $\lambda \in \mathbb{Q}$ we have that $\lambda v \in \mathbb{Z}^m$ implies that $\lambda v \in \Lambda$.

Let $\Lambda \subset \mathbb{Z}^m$ be a lattice with basis $u_1, \cdots, u_r$, and form the matrix B as above. Let $S = PBQ$ be its Smith normal form. Let S' be the matrix obtained from S by replacing all diagonal entries by 1. Set $B' = P^{-1}S'Q^{-1}$. Let Λ' be the lattice spanned by the rows of B'. Then Λ' is pure; in fact, it is the smallest pure lattice containing Λ. We call the lattice Λ' the saturation of Λ.

Proposition 8. $\Lambda \subset \mathbb{Z}^m$ is pure if and only if there is a basis $u_1, \cdots, u_m$ of $\mathbb{Z}^m$ such that $u_1, \cdots, u_r$ is a basis of Λ.

Proof. Let B be the $r \times m$-matrix corresponding to a basis of Λ. Let $S = PBQ$ be its Smith normal form. If Λ is pure, then S has 1-s on the diagonal. Hence the rows $u_1, ..., u_m$ of Q^{-1} are a basis of $\mathbb{Z}^m$ with the property that $1u_i \in \Lambda$ for $1 \leq i \leq r$. In other words, $u_1, \cdots, u_r$ is a basis of Λ.
For the converse, suppose that such a basis exists. Let $v \in \Lambda$ and $\lambda \in Q$ such that $\lambda v \in \mathbb{Z}^m$. Then $\lambda v = \sum_{i=1}^{m} \alpha_i u_i$, with $\alpha_i \in \mathbb{Z}$. But $v = \sum_{i=1}^{m} \beta_i u_i$. Hence $\alpha_i = 0$ for $i > r$, and $\lambda v \in \Lambda$.

□

The proof also gives a method to compute a basis as in the proposition. Indeed, we compute the Smith normal form $S = PBQ$ of B, and take the rows of Q^{-1}.

Corollary 1. Let $\Lambda_1 \subset \Lambda_2 \subset \mathbb{Z}^m$ be pure lattices of ranks $r_1 < r_2$. Then there exists a basis $u_1, \cdots, u_{r_2}$ of Λ_2 such that $u_1, \cdots, u_{r_1}$ is a basis of Λ_1.

Proof. By last proposition there exists a basis $v_1, \cdots, v_m$ of $\mathbb{Z}^m$ such that $v_1, \cdots, v_{r_2}$ is a basis of Λ_2. Now let $\sigma : \Lambda_2 \to \mathbb{Z}^{r_2}$ be the map sending a $v \in \Lambda_2$ to its coefficient vector with respect to this basis. Then σ is an isomorphism. Now $\sigma(\Lambda_1)$ is a pure lattice in $\mathbb{Z}^{r_2}$. So we get a basis $w_1, \cdots, w_{r_2}$ of $\mathbb{Z}^{r_2}$ such that $w_1, \cdots, w_{r_1}$ is a basis of $\sigma(\Lambda_1)$. Then the choice $u_i = \sigma^{-1}(w_i)$ does the job.

□

Here also the proof suggests a method for computing a basis as in the corollary. As seen above we can compute a basis $v_1, \cdots, v_m$ of $\mathbb{Z}^m$ such that $v_1, \cdots, v_{r_2}$ is a basis of Λ_2. Using that we compute the map σ and the lattice $\sigma(\Lambda_1) \subset \mathbb{Z}^{r_2}$. We compute a basis $w_1, \cdots, w_{r_2}$ of $\mathbb{Z}^{r_2}$ as in the proof, and map the w_i back.

In the section concerning cyclotomic fields and their unit group we give an example of how we use Ge's algorithm to compute a basis of a generating set of units.

2.3 Toral algebras

In this section we give some basis definitions about toral algebras and some constructive algorithms to see a toral algebra A as sum of field extensions of the rationals.

Definition 8. We say that an associative algebra A over $\mathbb{Q}$ is *toral* if it is semisimple, abelian and has an identity element, which we will denote by e. For example the algebra $\mathbb{Q}G$ of a finite abelian group G is toral.

By the Wedderburn structure theorem (cf. [25], §3.5) a toral algebra A is a direct sum $A := A_1 \oplus \cdots \oplus A_s$, where the A_i are ideals that are isomorphic (as associative algebra) to field extension of $\mathbb{Q}$.

Definition 9. A nonzero element $e_0 \in A$ is said to be an idempotent if $e_0^2 = e_0$. Two idempotents e_1,e_2 are called *orthogonal* if $e_1 e_2 = 0$. Furthermore, an idempotent is called *primitive* if it is not the sum of orthogonal idempotents.

Now, the decomposition of A into a direct sum of simple ideals correspond to a decomposition of the identity element $e \in A$ as sum of primitive orthogonal idempotents, $e = e_1 + \cdots + e_s$. Here e_i is the identity element of A_i, and vice versa $A_i = e_i A$. We describe now an algorithm to compute the e_i given a basis of A (cf. [16], [17]).

2.3.1 Splitting elements in toral algebras

Here we let K be a field of characteristic 0. By $M_n(K)$ we denote the associative algebra of $n \times n$-matrices with coefficients in K.

Definition 10. A subalgebra $T \subset M_n(K)$ is *toral* if it is semisimple and commutative. This is an equivalent definition as the one given before.

Definition 11. A subalgebra T is said to be toral if and only if its elements can simultaneously be diagonalized. The latter condition means that there is an extension field $F \supset K$ and an $X \in \mathrm{GL}_n(F)$ such that XTX^{-1} consists only of diagonal matrices.

In this subsection we review some algorithms for computing the structure of a toral algebra. For a more in-depth discussion of these matters we refer to [17] and [18].

Let $T \subset M_n(K)$ be toral, and suppose that T contains the identity. For $a \in T$ we write $K[a]$ for the subalgebra with one generated by a. An $a \in T$ is called a *splitting element* if $K[a] = T$. The next lemma, which is similar to the theorem of the primitive element in field theory, implies that splitting elements exist.

Lemma 2. Let $T \subset M_n(K)$ be toral, containing the identity. Write $m = \dim T$. Let $\Omega \subset K$ be a subset of size at least $\frac{m(m-1)}{2} + 1$. Let $a, b \in T$ be such that $a \notin K[b]$. Then there is an $\omega \in \Omega$ such that $\dim K[a + \omega b] > \dim K[b]$.

Proof. Let $F \supset K$ be an extension with the property that there is an element $X \in \mathrm{GL}_n(F)$ such that XTX^{-1} consists of diagonal matrices. For $i \leq i \leq n$ let $\alpha_i : T \to F$ be the function that maps $a \in T$ to the coefficient on position (i, i) of XaX^{-1}. Let $i_1, \ldots, i_s$ be such that the $\alpha_{i_k}(b)$ are exactly the distinct elements of the set $\{\alpha_i(b)\}$. Then the dimension of $K[b]$ is equal to s. (b is semisimple, so the number of distinct eigenvalues of b is equal to the degree of the minimal polynomial of b, which in turn is equal to $\dim K[b]$.) Moreover, we define a K-homomorphism $\phi : T \to M_s(F)$ by:

$$\phi(u) = \mathrm{diag}(\alpha_{i_1}(u), \ldots, \alpha_{i_s}(u)).$$

Restricted to $K[b]$, the map ϕ is injective. Suppose that $\alpha_i(b) = \alpha_j(b)$ implies that $\alpha_i(a) = \alpha_j(a)$. Then the restriction of ϕ to $K[a, b]$ is also injective, implying that $K[a, b] = K[b]$, which is a contradiction. So there are $i \neq j$ such that $\alpha_i(b) = \alpha_j(b)$ and $\alpha_i(a) \neq \alpha_j(a)$. Now consider the following equations in the unknown x:

$$\alpha_{i_k}(a) + x\alpha_{i_k}(b) = \alpha_{i_l}(a) + x\alpha_{i_l}(b), \text{ for } k < l.$$

Each equation has at most one solution in K. So since there are at most $\frac{m(m-1)}{2}$ such equations, there is an $\omega \in \Omega$ that is not a solution to any of them. Let $i \neq j$ be such that $\alpha_i(b) = \alpha_j(b)$ and $\alpha_i(a) \neq \alpha_j(a)$. Then it holds that $\alpha_i(a + \omega b) \neq \alpha_j(a + \omega b)$. Hence the number of distinct eigenvalues of $a + \omega b$ is strictly bigger than the number of distinct eigenvalues of b. Hence $\dim K[a + \omega b] > \dim K[b]$. □

Remark 2.3. We note that the lemma also yields a straightforward deterministic algorithm for computing a splitting element of T.

Next we indicate how a splitting element $a \in T$ yields the decomposition of T as a direct sum of simple ideals.

Let $f = p_1 \cdots p_s$ be the factorization of the minimal polynomial of a into distinct irreducible factors. For $1 \leq i \leq s$ let q_i be the product of all factors, except p_i. Then we have that $\gcd(q_1, \ldots, q_s) = 1$. So using the extended Euclidean algorithm we can compute polynomials h_i with $h_1q_1 + \cdots + h_sq_s = 1$. Now set $e_i = h_iq_i(a)$. Since f divides $h_iq_ih_jq_j$ we get $e_ie_j = 0$ for $i \neq j$. Moreover, the relation $e_1 + \cdots + e_s = 1$ implies $e_i = e_i(e_1 + \cdots + e_s) = e_i^2$. So the e_i are orthogonal idempotents.
Set $F_i = e_iT$. Then $T = F_1 \oplus \cdots \oplus F_s$ is a direct sum decomposition of T. Moreover, we have that $T = K[a] \cong K[x]/(f)$ which, by the chinese remainder theorem, is isomorphic to the direct sum of the algebras $K[x]/(p_i)$. So the decomposition of T cannot be further refined, and the F_i are field extensions of K.

2.3.2 Decomposition via irreducible character of G

When $A = \mathbb{Q}G$, with G a finite abelian group, there is a very efficient way to compute the primitive idempotents. Let $\chi : G \to \mathbb{C}^*$ be an irreducible character of G. Then

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

is an idempotent in $\mathbb{C}G$. Moreover, the e_χ, as χ runs over all irreducible characters, are primitive orthogonal idempotents with sum e (cf. [14], Theorem 33.8). In particular, they form a basis of $\mathbb{C}G$. Let m denote the exponent of G, then all irreducible characters χ have values in the cyclotomic field $\mathbb{Q}(\zeta_m)$. So the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ acts on the irreducible characters. Now we sum the e_χ, for χ in an orbit of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and obtain the primitive orthogonal idempotents of $\mathbb{Q}G$.

Definition 12. A subset $\mathcal{O}$ of a toral algebra A, containing the identity of A, is said to be an **order** (or, more precisely, a $\mathbb{Z}$-order) if there is a basis $a_1, \ldots, a_m$ of A such that $\mathcal{O} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_m$ and $a_i a_j \in \mathcal{O}$ for $1 \leq i, j \leq m$.

For example, $\mathbb{Z}G$ is an order in $\mathbb{Q}G$. The unit group of $\mathcal{O}$ is:

$$\mathcal{O}^* = \{a \in \mathcal{O} \mid \text{ there is } b \in \mathcal{O} \text{ with } ab = e\}.$$

We consider the problem of obtaining a basis of the lattice L of multiplicative relations.

$$L = \{(\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r \mid a_1^{\alpha_1} \cdots a_r^{\alpha_r} = e\},$$

where $a_1, \ldots, a_r$ are given elements of the group $\mathcal{O}^*$. Note that each $e_i A$ is number field. So using Ge's algorithm [4] we can compute basis of the lattices

$$L_j = \{(\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r \mid (e_j a_1)^{\alpha_1} \cdots (e_j a_r)^{\alpha_r} = e_j\}.$$

Moreover, $L = \cap_j L_j$ so we can compute a basis of L (see Section 2.2).

2.3.3 Standard generating sets

Definition 13. Let U be a finitely-generated abelian group. We say that a set of generators $g_1, \ldots, g_r$ of U is **standard** if:

1. for $1 \leq i \leq s$ the order of g_i is d_i,
2. for $s + 1 \leq i \leq r$ the order of g_i is infinite,
3. $d_i | d_{i+1}$ for $i < s$,

and there are no other relations.

So a standard set of generators immediately gives an isomorphism of U into the direct sum $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \mathbb{Z}^{r-s}$. Giving finitely-generated abelian groups by standard generating sets yields straightforward algorithms for several computational tasks concerning these groups, such as computing the index of a subgroup, and computing the kernel of a homomorphism.
If an abelian group is given by a non-standard set of generators, then we can compute a standard one by computing the lattice of all relations of the generators, followed by

a Smith normal form computation (cf. [28], §8.3). So, using the algorithm indicated in the previous section, we can compute a standard set of generators for a finitely-generated subgroup of $\mathcal{O}^*$, where $\mathcal{O}$ is an order in a toral algebra.
For many computational problems regarding finitely-generated abelian groups it suffices to compute a Hermite normal form of the relation lattice. However, in our applications the main computational problem is to obtain the relation lattice the subsequent computation of the Smith normal form does not bear heavily on the running time. Therefore, for our purposes, a Smith normal form is the most convenient.

2.4 Cyclotomic fields $\mathbb{Q}(\zeta_n)$

Wedderburn's structure theorem says that every toral algebra A is isomorphic to a direct sum of number fields $F_1 \oplus \cdots \oplus F_r$. When $A = \mathbb{Q}G$ with G abelian those number fields are cyclotomic fields $\mathbb{Q}(\zeta)$. So $A \cong \mathbb{Q}(\zeta_{n_1}) \oplus \cdots \oplus \mathbb{Q}(\zeta_{n_r})$. We also know that using this isomorphism (ψ) we have that $\psi((\mathbb{Z}G)^*)$ has finite index in the group of units of that direct sum of cyclotomic fields. So in order to compute $(\mathbb{Z}G)^*$ we need to be able to compute $\mathbb{Z}[\zeta_{n_i}]^*$.
How can we obtain generators of the unit group, $\mathbb{Z}[\zeta_n]^*$? There are algorithms for this that work for any number field (cf. [2]); but their complexity is such that it is only practical to use them for n up to about 20 (depending on the hardware one uses, of course). For this reason, we sketch a different approach, using several results from the literature. The situation is straightforward when n is a prime power, see Section 2.4.1. Then in Section 2.4.2 we describe what can be done when n is not a prime power. Using these methods we obtained a list of the generators of the unit groups $\mathbb{Z}[\zeta_n]^*$, for $n < 130$. However, for several n the correctness of this list depends on the Generalized Riemann Hypothesis, that is for n prime between 67 and 127, and for $n = 115, 119, 121, 123, 125, 129$ (so 19 cases in total).

Theorem 5. Let n be a positive integer, not equal to $2 \bmod 4$. Consider the cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. Then the ring of integers of this field is $\mathbb{Z}[\zeta_n]$ and the unit group $\mathbb{Z}[\zeta_n]^*$ is equal to $T \times F$, where F is a free abelian group of rank $\frac{1}{2}\varphi(n) - 1$, and T is the group of roots of unity of $\mathbb{Q}(\zeta_n)$.

Throughout we set $\mathbb{Q}(\zeta_n)^+ = \mathbb{R} \cap \mathbb{Q}(\zeta_n)$; then $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. By h_n^+ we denote the class number of $\mathbb{Q}(\zeta_n)^+$.

2.4.1 When n is a prime power

Suppose that $n = p^m$ is a prime power. For $1 < a < \frac{n}{2}$ with $\gcd(a, p) = 1$ set

$$\xi_a = \zeta_n^{\frac{1-a}{2}} \frac{1 - \zeta_n^a}{1 - \zeta_n}.$$

Then ξ_a lies in the unit group of $\mathbb{Q}(\zeta_n)^+$. Let U_n be the group generated by -1, ζ_n and all ξ_a. Then for the index we have $[\mathbb{Z}[\zeta_n]^* : U_n] = h_n^+$ (this is obtained by combining Corollary 4.13, Lemma 8.1 and Theorem 8.2 in [29]). For small n it is known that $h_n^+ = 1$: if $\varphi(n) < 66$, and if $\varphi(n) < 162$ assuming the Generalized Riemann Hypothesis (see the Appendix in [29]). So for those n we have generators of the unit group.

2.4.2 When n is not a prime power

Here the situation is more difficult. First of all we assume that $n \neq 2 \bmod 4$, as for $n = 2 \bmod 4$ we have that $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_{\frac{n}{2}})$ are isomorphic. By E^+ denote the unit group of $\mathbb{Q}(\zeta_n)^+$. We use a finite-index subgroup of E^+ defined by Greither [19]. Here we briefly describe his construction.
Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, and write the elements of G as σ_a, where $\gcd(a, n) = 1$ and $\sigma_a(\zeta_n) = \zeta_n^a$. For $\alpha = \sum_a m_a \sigma_a \in \mathbb{Z}G$ and $x \in \mathbb{Q}(\zeta_n)$ define:

$$x^\alpha = \prod_a \sigma_a(x)^{m_a}.$$

Let $n = \prod_{i=1}^s p_i^{e_i}$ be the factorization of n in distinct prime powers. Set $S = \{1, \ldots, s\}$ and $P_S = \{I \subset S \mid I \neq S\}$. For $I \in P_S$ we set $n_I = \prod_{i \in I} p_i^{e_i}$.
We consider arbitrary maps $\beta : S \to \mathbb{Z}G$, which we extend to maps (denoted by the same symbol) $\beta : P_S \to \mathbb{Z}G$ by:

$$\beta(\emptyset) = 1, \;\; \beta(\{i\}) = \beta(i), \text{ and } \beta(I \cup J) = \beta(I)\beta(J) \text{ if } I \cap J = \emptyset.$$

Now let $z \in \mathbb{Q}(\zeta_n)$. For $I \in P_S$ set $z_I = 1 - z^{n_I}$, and $z(\beta) = \prod_{I \in S} z_I^{\beta(I)}$.
Set $t = -\sum_{I \in S} n_I \beta(I) \in \mathbb{Z}\mathcal{G}$. Then for a with $1 < a < \frac{n}{2}$ and $\gcd(a, n) = 1$ we consider:

$$\xi_a(\beta) = \zeta_n^{d_a} \frac{\sigma_a(z(\beta))}{z(\beta)}, \text{ where } d_a = \frac{(1 - \sigma_a)t}{2}.$$

(Note that for n odd, $\zeta_n^{\frac{1}{2}}$ lies in $\mathbb{Z}[\zeta_n]$, whereas for n even we have a odd and hence $\frac{1-a}{2}$ is an integer.) Following Greither we describe a good choice for β.
First a small piece of notation: if g is an element of order m of a group, then we set $N_g = 1 + g + \cdots + g^{m-1}$, which lies in the corresponding integral group ring. Now consider an $i \in S$. Let G_i denote the Galois group of $\mathbb{Q}(\zeta_{n/p_i^{e_i}})^+$ over $\mathbb{Q}$. This group contains the Frobenius automorphism F_i (by definition: $F_i(\zeta_{n/p_i^{e_i}}) = \zeta_{n/p_i^{e_i}}^{p_i}$). This yields the element N_{F_i} in $\mathbb{Z}G_i$. Now we define $\beta(i)$ to be a lift of N_{F_i} to $\mathbb{Z}\mathcal{G}$.
Let C_β be the subgroup of E^+ generated by -1 and the $\xi_a(\beta)$. Greither proved that C_β does not depend on the choice for the lifts of the N_{F_i}, and that it is of index $h_n^+ i_\beta$ in E^+, where

$$i_\beta = \prod_{i=1}^s e_i^{g_i - 1} f_i^{2g_i - 1};$$

here e_i, f_i and g_i are respectively the ramification, inertial and decomposition degree of p_i in $\mathbb{Q}(\zeta_n)^+$ (so that $e_i f_i g_i = \frac{1}{2}\varphi(n)$). Now let U_n denote the group generated by ζ_n and the group C_β. Then using [29], Corollary 4.13, we get that $[\mathbb{Z}[\zeta_n]^* : U_n] = 2h_n^+ i_\beta$.

2.4.3 Explicit Construction of Greither 's Units

Now, we will show an example of the construction of Greither's units when $n = 15$. In this case we can work in $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ instead of $Gal(\mathbb{Q}(\zeta_n)^+/\mathbb{Q})$.

Let K be $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$, where ζ_{15} is a 15-th primitive root of unity. Observe that:

$$15 = \prod_{i=1}^2 p_i^{e_i} = 3^1 \times 5^1 \text{ and } \phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 8;$$

hence:

$$G_0 = Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \equiv U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

where we identified $\sigma_i \in G_0$ with $i \in U_{15}$, and we have that $\sigma_i(\zeta) = i(\zeta) = \zeta^i$.
It also holds that:

- $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{15}) : \mathbb{Q}(\zeta_5)][\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 2 \times 4 = 8$
- $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{15}) : \mathbb{Q}(\zeta_3)][\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 4 \times 2 = 8$

And these ones are all the possibly chains of intermediate fields. In order to apply Greither 's construction, let $S = \{1, 2\}$ so $P_S = \{\{1\}, \{2\}, \emptyset\}$, and let $p_1 = 3$ and $p_2 = 5$. Our aim is to construct a multiplicative function $\beta : P_S \to \mathbb{Z}G_0$, by using opportune lifting of N_{F_i} to $\mathbb{Z}G_0$.

Let us work with $p_1 = 3$.
First we have to find the order of $F_1 = Frob_3$, the Frobenius automorphism of exponent 3, in $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$.

- $F_1(\zeta_5) = \zeta_5^3$;
- $F_1^2(\zeta_5) = F_1(\zeta_5^3) = F_1(\zeta_5)^3 = \zeta_5^9 = \zeta_5^{-1}$,
- $F_1^3(\zeta_5) = F_1(\zeta_5)^{-1}) = F_1(\zeta_5)^{-1} = \zeta_5^{-3}$
- $F_1^4(\zeta_5) = F_1(\zeta_5)^{-3}) = F_1(\zeta_5)^{-3} = \zeta_5^{-9} = \zeta_5 = Id(\zeta_5)$

So the order of F_1 is 4. Hence it follows that: $N_{F_1} = 1 + F_1 + F_1^2 + F_1^3$. We now have to find a lifting of F_1 to G_0 and we will use some Galois theory for that purpose. We know that, since G_0 is a cyclic group, it is abelian, so every subgroup is normal and hence it makes sense to take the quotient. Let:

$$H = \{i \in U_{15} \mid i \equiv 1 \pmod 5\} = \{1, 11\};$$

this is a subgroup of G_0 isomorphic to $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q})$. So it follows that the quotient group $G_1 = G_0/H \equiv \{H, 2H, 4H, 8H\}$ is isomorphic to $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$.
To find a lifting of F_1 it suffices to choose an element t of G_1 such that we have $t(\zeta_5) = F_1(\zeta_5)$. We have:

- $1(\zeta_5) = \zeta_5$
- $2(\zeta_5) = \zeta_5^2$
- $4(\zeta_5) = \zeta_5^4$
- $8(\zeta_5) = \zeta_5^8 = \zeta_5^3 = F_1(\zeta_5)$

So a lifting of F_1 is 8 or, better, σ_8. Therefore we have:

$$\beta(\{1\}) = \beta(1) = 1 + \sigma_8 + \sigma_8^2 + \sigma_8^3 = 1 + \sigma_8 + \sigma_4 + \sigma_2.$$

Let us work with $p_2 = 5$.
First we have to find the order of $F_2 = Frob_5$, the Frobenius automorphism of exponent 5, in $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}$.

- $F_2(\zeta_3) = \zeta_3^5 = \zeta_3^2 = Id(\zeta_3)$;
- $F_2^2(\zeta_3) = F_2(\zeta_3^2) = F_2(\zeta_3)^2 = \zeta_3^{10} = \zeta_3 = Id(\zeta_3)$;

So the order of F_2 is 2. Hence it follows that: $N_{F_2} = 1 + F_2$. We now have to find a lifting of F_2 to G_0 and we will use again some Galois theory for that purpose. We know that, since G_0 is a cyclic group, it is abelian, so every subgroup is normal and hence it makes sense to take the quotient. Let:

$$H = \{i \in U_{15} \mid i \equiv 1 \pmod 3\} = \{1, 4, 7, 13\};$$

this is a subgroup of G_0 isomorphic to $Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. So it follows that the quotient group $G_2 = G_0/H \equiv \{H, 2H\}$ is isomorphic to $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q})$. To find a lifting of F_2 it suffices to choose an element t of G_2 such that $t(\zeta_3) = F_2(\zeta_3)$. We have:

- $1(\zeta_3) = \zeta_3$
- $2(\zeta_3) = \zeta_3^2 = \zeta_3^5 = F_2(\zeta_3)$

So a lifting of F_2 is 2 or, better, σ_2. Therefore we have:

$$\beta(\{2\}) = \beta(2) = 1 + \sigma_2$$

Greither 's construction.
We have defined our multiplicative function $\beta : P_S \to \mathbb{Z}G_0$ as:

- $\beta(\emptyset) = 1$
- $\beta(1) = 1 + \sigma_8 + \sigma_4 + \sigma_2$
- $\beta(2) = 1 + \sigma_2$

To not make the notation too heavy we put $\zeta = \zeta_{15}$ We have:

1. $n_\emptyset = 1, \quad n_1 = 3, \quad n_2 = 5$
2. $z_\emptyset = 1 - \zeta, \quad z_1 = 1 - \zeta^3, \quad z_2 = 1 - \zeta^5$
3. $z(\beta) = \prod_{I \in P_S} z_I^{\beta(I)} = z_\emptyset^{n_\emptyset} z_1^{n_1} z_2^{n_2} =$
   $= (1-\zeta)^1 (1-\zeta_{15})^{1+\sigma_8+\sigma_4+\sigma_2} (1-\zeta^5)^{1+\sigma_2} =$
   $= (1-\zeta)(1-\zeta^3)(1-\zeta^6)(1-\zeta^{12})(1-\zeta^9)(1-\zeta^5)(1-\zeta^{10})$
4. $t = \sum_{I \in P_S} n_I \beta(I) = 1 + 3(1 + \sigma_8 + \sigma_4 + \sigma_2) + 5(1 + \sigma_2) \equiv 1 \mod 15$

We also observe that $n/2 = 7.5$, hence we have to work only with
$a \in \{2, 4, 7\}$. We have:

- $\sigma_2(z(\beta)) = \sigma_2((1-\zeta)(1-\zeta^3)(1-\zeta^6)(1-\zeta^{12})(1-\zeta^9)(1-\zeta^5)(1-\zeta^{10})) =$
  $= (1-\zeta^2)(1-\zeta^6)(1-\zeta^12)(1-\zeta^{24})(1-\zeta^{18})(1-\zeta^10)(1-\zeta^{20}) =$
  $= (1-\zeta^2)(1-\zeta^6)(1-\zeta^12)(1-\zeta^9)(1-\zeta^3)(1-\zeta^10)(1-\zeta^5)$

- $\sigma_4(z(\beta)) = \sigma_4((1-\zeta)(1-\zeta^3)(1-\zeta^6)(1-\zeta^{12})(1-\zeta^9)(1-\zeta^5)(1-\zeta^{10})) =$
  $= (1-\zeta^4)(1-\zeta^12)(1-\zeta^9)(1-\zeta^3)(1-\zeta^6)(1-\zeta^5)(1-\zeta^{10})$
- $\sigma_7(z(\beta)) = \sigma_7((1-\zeta)(1-\zeta^3)(1-\zeta^6)(1-\zeta^{12})(1-\zeta^9)(1-\zeta^5)(1-\zeta^{10})) =$
  $= (1-\zeta^7)(1-\zeta^6)(1-\zeta^{12})(1-\zeta^9)(1-\zeta^3)(1-\zeta^5)(1-\zeta^{10}))$

The Greither 's units are:

- $\xi_2(\beta) = \zeta^{\frac{(1-\sigma_2)t}{2}} \frac{\sigma_2(z(\beta))}{z(\beta)} = -2\zeta^7 + \zeta^5 - \zeta^4 + \zeta^3 - \zeta + 1$
- $\xi_4(\beta) = \zeta^{\frac{(1-\sigma_4)t}{2}} \frac{\sigma_4(z(\beta))}{z(\beta)} = \zeta^5 + -\zeta^4 - \zeta^3 + 2\zeta^2 - \zeta$
- $\xi_7(\beta) = \zeta^{\frac{(1-\sigma_7)t}{2}} \frac{\sigma_7(z(\beta))}{z(\beta)} = -\zeta^6 + \zeta^4 - \zeta$

Hence our subgroup C_β is $\langle -1,\ \xi_2(\beta),\ \xi_4(\beta),\ \xi_7(\beta)\rangle$ Let's calculates its index in the group of units E_{15}^+. We first have to find for each i the parameters f_i, g_i, e_i. From a previous remark we know that $f_i g_i e_i = [\mathbb{Q}(\zeta_{15})^+] = \phi(15)/2 = 4$, and we also know that if $s \geq 2$ then $e_i = \phi(p_i^{e_i})$, so:

$$e_1 = \phi(3) = 2 \text{ and } e_2 = \phi(5) = 4.$$

Thanks to MAGMA, we computed the factorization in $\mathbb{Q}(\zeta_{15})^+$ of the ideals $\langle 3\rangle\mathcal{O}$ and $\langle 5\rangle\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\zeta_{15})^+$ We obtain:

- $\langle 3\rangle\mathcal{O} = P_1^2$
- $\langle 5\rangle\mathcal{O} = P_2^4$

where, P_i are prime ideals of $\mathbb{Q}(\zeta_{15})^+$. Since the g_i represent the number of factors, we have $g_1 = g_2 = 1$. Hence $f_1 = 2$ and $f_2 = 4$, so:

$$i_\beta = \prod_{i=1}^{s} e_i^{g_i - 1} f_i^{2g_i - 1} = 2^0 2^1 4^0 1^1 = 2$$

Now we will use the algorithms presented before, to try to find the full group of units of $\mathbb{Q}(\zeta_n)$ for some n. The Greither units are :

$$C_\beta = \{-2\zeta^7 + \zeta^5 - \zeta^4 + \zeta^3 - \zeta + 1, \zeta^5 + -\zeta^4 - \zeta^3 + 2\zeta^2 - \zeta, -\zeta^6 + \zeta^4 - \zeta, -1\}$$

We write $C_\beta = \{w_1, w_2, w_3, w_4\}$. So the subgroup H of E_{15} we start from is $H = \langle C_\beta, \zeta_n\rangle = \langle w_1, w_2, w_3, w_4, w_5\rangle$. Therefore group G is:

$$G = \langle C_\beta \cup \{\zeta_{15}\} \cup \{a_i \doteq 1 - \zeta_{15}^i \mid (i, 15) = 1\}\rangle$$

and we write $G = \langle w_1, w_2, w_3, w_4, w_5, a_1, a_2, a_4, a_7, a_8, a_{11}, a_{13}, a_{14}\rangle$

So, G is generated by these elements, but they are not independent generators of $\mathcal{G}$. The multiplicative relationships between them are:

w_1	w_2	w_3	w_4	w_5	a_1	a_2	a_4	a_7	a_8	a_{11}	a_{14}	a_{14}
1	0	0	0	0	0	0	0	1	14	15	14	16
0	1	0	0	0	0	0	0	0	3	4	3	2
0	0	1	0	0	0	0	0	1	7	7	7	6
0	0	0	1	0	0	0	0	1	0	1	1	1
0	0	0	0	1	0	0	0	0	13	13	13	13
0	0	0	0	0	1	0	0	1	13	14	14	13
0	0	0	0	0	0	1	0	1	11	12	11	12
0	0	0	0	0	0	0	1	1	7	7	8	8
0	0	0	0	0	0	0	0	2	0	2	2	2
0	0	0	0	0	0	0	0	0	15	15	15	15

Viewed as matrix B its Normal Smith Form S is:

$$S = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 30 & 0 & 0 & 0 \end{vmatrix}$$

So G is spanned by the rows of Q^{-1}:

$$Q^{-1} = \begin{vmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 4 & 3 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 13 & 13 & 13 & 13 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 14 & 15 & 14 & 16 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 7 & 7 & 7 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 13 & 14 & 14 & 13 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 11 & 12 & 11 & 12 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 7 & 7 & 8 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -14 & 15 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

Note Q^{-1} is spanned from its last four rows, i.e, the product of the associate units are the independent generators of G. Hence G is generated by $g_1 = (a_7^{-1} \cdot a_8)$, $g_2 = a_{11}$, $g_3 = a_{13}$, $g_4 = a_{14}$. Let us compute the index of G in H.

The the matrix P of the multiplicative relations is:

$$P = \begin{vmatrix} 29 & 0 & -1 & 1 \\ 18 & 1 & 0 & -1 \\ 7 & -1 & -1 & -2 \\ 15 & 0 & 0 & 0 \\ 28 & 0 & 0 & 0 \end{vmatrix}$$

That means that:

- $w_1 = g_1^{29} \cdot g_2^0 \cdot g_3^{-1} \cdot g_4^1$
- $w_2 = g_1^{18} \cdot g_2^1 \cdot g_3^0 \cdot g_4^{-1}$
- $w_3 = g_1^7 \cdot g_2^7 \cdot g_3^{-1} \cdot g_4^0$
- $w_4 = g_1^{15} \cdot g_2^0 \cdot g_3^0 \cdot g_4^0$
- $w_5 = g_1^{28} \cdot g_2^0 \cdot g_3^0 \cdot g_4^0$

The matrix J of the Hermite form of P is:

$$J = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{vmatrix}$$

Hence, the index $[G : H] = 1 \cdot 1 \cdot 1 \cdot 4 = 4$.
From a previous section we know that the index:

$$[E_{15} : H] = 2 \cdot h_{15}^+ \cdot i_\beta = 4.$$

So in this case, since we have found a subgroup G of E_{15} whose index in H is 4, we found the full group of units.

2.4.4 Fieker's program

Greither's construction is very useful but it does not always give the whole group of units of the cyclotomic filed. In those cases we need to find more units to enlarge our subgroup. The only thing that we know are how big our group need to be and we know the prime dividing the index $[E_{15} : H] = 2 \cdot h_{15}^+ \cdot i_\beta$.
To solve this problem we used a program that Claus Fieker has written in MAGMA, V2.17-2. This program, given a finite-index subgroup V of $\mathbb{Z}[\zeta_n]^*$, and a prime p, computes a subgroup $\widetilde{V}$ of $\mathbb{Z}[\zeta_n]^*$, containing V, and such that the index $[\mathbb{Z}[\zeta_n]^* : \widetilde{V}]$ is not divisible by p. We used this starting with the group U_n. For $n < 130$ and $\varphi(n) \leq 72$ we have $h_n^+ = 1$, and assuming the Generalized Riemann Hypothesis, we have $h_n^+ = 1$ for all $n < 130$ ([29], Appendix). Therefore we can compute $[\mathbb{Z}[\zeta_n]^* : U_n]$, and get all primes dividing it. So in the end we arrived at the full unit group $\mathbb{Z}[\zeta_n]^*$ for all $n < 130$.

2.5 Unit groups of orders in toral matrix algebras

This section contains the main algorithm of the paper we published, namely an algorithm for computing the unit group of an order $\mathcal{O}$ in a toral algebra A. The main idea is to split A into its simple ideals e_iA where the e_i are the orthogonal primitive idempotents. The e_iA are number fields with orders $e_i\mathcal{O}$. So in order to compute their unit group we can use the effective version of the Dirichlet unit theorem (see [2], [26]). The basic step of the algorithm is, given two orthogonal idempotents e_1, e_2, to obtain the unit group of $(e_1 + e_2)\mathcal{O}$ given the unit group of $e_i\mathcal{O}$, $i = 1, 2$.

Let A be a toral algebra with identity e, and $\mathcal{O} \subset A$ an order. First we consider some special cases.

2.5.1 A simple toral algebra

Let A be a simple toral algebra. In other words, it is isomorphic to a finite extension of $\mathbb{Q}$. Now there are algorithms for computing generators of an order in a number field (the effective version of the Dirichlet unit theorem, see [2], [26]). We use these to compute generators of $\mathcal{O}^*$ as well.

2.5.2 Two idempotents

Let A be a toral algebra with identity e, and $e_1, e_2 \in A$ orthogonal (but not necessarily primitive) idempotents with $e_1 + e_2 = e$. Set $A_i = e_iA$, then $A = A_1 \oplus A_2$. Let $\mathcal{O}$ be an order in A, then $\mathcal{O}_i = e_i\mathcal{O}$ is an order in A_i. Here we suppose that we have generators of $\mathcal{O}_i^*$, $i = 1, 2$, and the problem is to find generators of $\mathcal{O}^*$.
Set $J = (e_1\mathcal{O} \cap \mathcal{O}) + (e_2\mathcal{O} \cap \mathcal{O})$. Since this is an ideal in $\mathcal{O}$ we can form the quotient $R = \mathcal{O}/J$. Consider the maps $\varphi_i : e_i\mathcal{O} \to R$ defined by $\varphi_i(e_ia) = a + J$, for $a \in \mathcal{O}$. (Note that this is well-defined: if $e_1a = e_1b$ then $a - b = e_2(a - b)$ so it lies in J.) These are surjective ring homomorphisms with respective kernels $e_i\mathcal{O} \cap \mathcal{O}$.

Lemma 3. $\mathcal{O} = \{a_1 + a_2 \mid a_i \in e_i\mathcal{O} \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$.

Proof. Let $a \in \mathcal{O}$ and set $a_i = e_ia$ then $a = a_1 + a_2$ and $a_i \in e_i\mathcal{O}$. Moreover $\varphi_1(a_1) = a + J = \varphi_2(a_2)$. Conversely, let $a, b \in \mathcal{O}$ be such that $\varphi_1(a_1) = \varphi_2(a_2)$, where $a_1 = e_1a$ and $a_2 = e_2b$. Then $a - b \in J$, whence $a = b + u_1 + u_2$ where $u_i \in e_i\mathcal{O}\cap\mathcal{O}$. Therefore $e_1a = e_1b+u_1$ so that $a_1+a_2 = e_1a+e_2b = e_1b+e_2b+u_1 = b+u_1$ which lies in $\mathcal{O}$. □

Corollary 2. $\mathcal{O}^* = \{a_1 + a_2 \mid a_i \in (e_i\mathcal{O})^* \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$.

So in order to compute generators of $\mathcal{O}^*$ we perform the following steps:

1. Compute bases of $\mathcal{O}_i = e_i\mathcal{O}$.
2. Compute bases of $\mathcal{O}_i \cap \mathcal{O}$, of $J = (\mathcal{O}_1 \cap \mathcal{O}) + (\mathcal{O}_2 \cap \mathcal{O})$, and set $R = \mathcal{O}/J$.
3. Compute generators of the groups $H_i = \varphi_i(\mathcal{O}_i^*) \subset R^*$ and $H = H_1 \cap H_2$.
4. Compute generators of the groups $M_i = \varphi_i^{-1}(H) \subset \mathcal{O}_i^*$.
5. Compute generators of the group $\mathcal{O}^* = \{a_1 + a_2 \mid a_i \in M_i \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$.

2.5.3 Implementation

We comment on the implementation of the steps of the algorithm. Step (1) is done by a Hermite normal form computation. The intersections in Step (2) are computed using the techniques indicated in Section 2.2. Note that a basis of J is obtained by concatenating the bases of $\mathcal{O}_i \cap \mathcal{O}$. The ring $R = \mathcal{O}/J$ can be constructed by a Smith normal form computation.
For Step (3) we assume that $e_2 A$ is isomorphic to a number field (in other words, that e_2 is a primitive idempotent). When using the algorithm, this can always be arranged (see Section 2.5.4). Then $e_2\mathcal{O}$ an order in it. We set $I = e_2\mathcal{O} \cap \mathcal{O}$ and use the isomorphism $R \cong (e_2\mathcal{O})/I$. Subsequently we use algorithms described in [20], [24] to compute a standard generating set of $(e_2\mathcal{O}/I)^*$. So computing H_1, H_2 as subgroups of $(e_2\mathcal{O}/I)^*$ we can perform the operations of Step (3).
In Step (4) we view φ_i as a homomorphism $\mathcal{O}_i^* \to H_i$. We use this to compute generators of the kernel of φ_i as well as pre-images of the generators of H. Together these generate the group M_i. As remarked in Section 2.3.3, we can compute standard generating sets of the groups $\mathcal{O}_i^*$. Using these, it is straightforward to obtain a standard generating set for the subgroups M_i. Then we restrict φ_i to obtain a homomorphism $\varphi_i : M_i \to H$.
Now we come to Step (5). Let $h_1, \ldots, h_r, a_1, \ldots, a_s, b_1, \ldots, b_t$ be standard generating sets of H, M_1 and M_2 respectively. Set

$$\Lambda = \{(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \mathbb{Z}^{s+t} \mid \varphi_1(a_1^{\alpha_1} \cdots a_s^{\alpha_s}) = \varphi_2(b_1^{\beta_1} \cdots \beta_t^{e_t})\}.$$

Then:

$$\mathcal{O}^* = \{a_1^{\alpha_1} \cdots a_s^{\alpha_s} + b_1^{\beta_1} \cdots b_t^{\beta_t} \mid (\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \Lambda\}.$$

Moreover, Λ is a lattice, hence has a finite basis. Furthermore, the elements of $\mathcal{O}^*$ corresponding to the elements of a basis of Λ generate $\mathcal{O}^*$. So the problem of finding a generating set of $\mathcal{O}^*$ is reduced to finding a basis of Λ.
Define $\mu_{ij}, \nu_{ij} \in \mathbb{Z}$ by

$$\varphi_1(a_i) = \prod_{j=1}^{r} h_j^{\mu_{ij}}$$
$$\varphi_2(b_i) = \prod_{j=1}^{r} h_j^{\nu_{ij}}.$$

A small calculation shows that $(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \Lambda$ if and only if

$$\sum_{i=1}^{s} \mu_{ij}\alpha_i - \sum_{k=1}^{t} \nu_{kj}\beta_k = 0 \bmod \mathrm{ord}(h_j) \tag{2.1}$$

for $1 \leq j \leq r$ (and where $\mathrm{ord}(h_j)$ denotes the order of h_j). Let S be the integral matrix with columns

$$(\mu_{1j}, \ldots, \mu_{sj}, -\nu_{1j}, \ldots, -\nu_{tj}, \mathrm{ord}(h_j))$$

for $1 \leq j \leq r$. We compute a basis the integral kernel of S, which is the set of all $v \in \mathbb{Z}^{s+t+1}$ such that $vS = 0$. For each v in this basis we take the vector consisting of the first $s + t$ coordinates. This way we obtain a basis of Λ.

2.5.4 The general case

Now let A be a toral algebra, $e_1, \ldots, e_m$ its primitive orthogonal idempotents with sum e, and $A_i = e_i A$ the corresponding simple ideals. Let $\mathcal{O}$ be an order in A; then $e_i\mathcal{O}$ is an order in A_i, and as indicated in Section 2.5.1, we can compute generators of the unit groups $(e_i\mathcal{O})^*$. Then for $j = 2, 3, \ldots$ we set $\varepsilon_j = e_1 + \cdots + e_j$ and we apply the algorithm of Section 2.5.2 to the algebra $\varepsilon_j A$ with its order $\varepsilon_j\mathcal{O}$, and two idempotents ε_{j-1} and e_j, yielding the unit group $(\varepsilon_j\mathcal{O})^*$. When the algorithm terminates we have the unit group $\mathcal{O}^*$.

2.6 Units of integral abelian group rings

Let G be an abelian group. As seen in Section 2.3.1, it is straightforward to compute primitive orthogonal idempotents $e_1, \ldots, e_r \in \mathbb{Q}G$ such that $e_i(\mathbb{Q}G)$ is isomorphic to a field extension of $\mathbb{Q}$. Let m denote the exponent of G, then (cf. [10])

$$\mathbb{Q}G \cong \bigoplus_{d|m} \bigoplus_{i=1}^{t_d} \mathbb{Q}(\zeta_d),$$

where $\mathbb{Q}(\zeta_d)$ is the cyclotomic field of order d, and t_d is the number of cyclic subgroups of G of order d. In particular, $e_i(\mathbb{Q}G) \cong \mathbb{Q}(\zeta_{d_i})$. We consider the order $\mathbb{Z}G$ in $\mathbb{Q}G$. We have that $e_i(\mathbb{Z}G)$ is isomorphic to $\mathbb{Z}[\zeta_{d_i}]$, and by the results of Section 2.4, we have generators of $\mathbb{Z}[\zeta_{d_i}]^*$ for $d_i < 130$. So for small groups G we can apply the algorithm of Section 2.5 to obtain generators of the unit group $(\mathbb{Z}G)^*$. Using our implementation of the algorithms in MAGMA, we have carried this out for all abelian groups of orders up to 110. In Table 2 we collect some timings and other data related to the algorithm.

G	$\varphi(\exp(G))$	|digits|	t_m	t_{tot}
C_{70}	24	7.4	314	328
C_{80}	32	63.4	1131	1183
C_{90}	24	159.5	1043	1078
C_{91}	72	3.7	2352	2446
C_{96}	32	31.2	2322	2373
$C_2 \times C_{48}$	16	181.3	1575	1781
$C_2 \times C_2 \times C_{24}$	8	54.6	1031	1267
$C_2 \times C_4 \times C_{12}$	4	22.5	537	725
C_{100}	40	217.6	3822	3942
$C_2 \times C_{50}$	20	66352.6	414569	426654
$C_5 \times C_{20}$	8	379.7	1227	1425
$C_{10} \times C_{10}$	4	275.2	1131	1332

Table 2: Runtimes (in seconds) for the algorithm to compute generators of $(\mathbb{Z}G)^*$. The first column lists the isomorphism type of G, and the second the value of the Euler φ-function on the exponent of G. The third column has the average number of digits of the coefficients of the units output by the algorithm (with respect to the standard basis of $\mathbb{Z}G$). The fourth column displays the time spent to compute multiplicative relations in cyclotomic fields. The last column has the total time spent by the algorithm.

From Table 2, we see that the running time is dominated by the time needed to compute multiplicative relations in cyclotomic fields (Ge's algorithm). This algorithm needs to work harder if the degrees of the fields that occur are higher. Indeed, the Runtimes generally increase when $\varphi(\exp(G))$ increases (note that this is the highest degree of a cyclotomic field occurring in the decomposition of $\mathbb{Q}G$). However, also the size of the elements of which we need to compute multiplicative relations plays a role. For some groups the average number of digits of a unit, as output by the algorithm, is very high. This is seen most dramatically for $C_2 \times C_{50}$. Note also that the size (i.e., the average number of digits of their coefficients) of the units output by the algorithm is far from being optimal; indeed, for $G = C_2 \times C_{50}$, the unit group $(\mathbb{Z}G)^*$ is also generated by the Hoechsmann units (see below).

We let $\mathrm{Hind}(G)$ be the index of $\mathcal{H}$ in $(\mathbb{Z}G)^*$, and we call this number the Hoechsmann index. We have computed the Hoechsmann indices for all abelian groups of orders up to 110. For most groups the index is 1. The groups for which it is not 1 are listed in Table 3, along with the corresponding Hoechsmann indices.

From Table 3 we see that on many occasions when $\mathrm{Hind}(G) \neq 1$ we have that $|G| = m$, with H_m not cyclic. Also, for the groups considered, if for one group G of order m we have $\mathrm{Hind}(G) \neq 1$, then the same holds for all groups of that order (except when $(\mathbb{Z}G)^*$ has rank 0).

G	$\mathrm{Hind}(G)$	G	$\mathrm{Hind}(G)$
C_{40}	2	C_{84}	2
$C_2 \times C_{20}$	2	$C_2 \times C_{42}$	2
$C_2 \times C_2 \times C_{10}$	2	C_{85}	2
C_{48}	2	C_{90}	3
$C_2 \times C_{24}$	2	$C_3 \times C_{30}$	3
$C_2 \times C_2 \times C_{12}$	2	C_{91}	3
$C_4 \times C_{12}$	4	C_{96}	8
C_{60}	2	$C_2 \times C_{48}$	16
$C_2 \times C_{30}$	2	$C_2 \times C_2 \times C_{24}$	32
C_{63}	3	$C_2 \times C_2 \times C_2 \times C_{12}$	16
$C_3 \times C_{21}$	3	$C_2 \times C_4 \times C_{12}$	64
C_{65}	2	$C_4 \times C_{24}$	64
C_{74}	3	C_{98}	7
C_{80}	4	$C_7 \times C_{14}$	343
$C_2 \times C_{40}$	8	C_{104}	2
$C_2 \times C_2 \times C_{20}$	16	$C_2 \times C_{52}$	2
$C_2 \times C_2 \times C_2 \times C_{10}$	32	$C_2 \times C_2 \times C_{26}$	2
$C_4 \times C_{20}$	8	C_{105}	4

Table 3: Hoechsmann indices for abelian groups of orders up to 110, for which this index is not 1.

Remark 2.4. For the groups C_p, with p a prime between 67 and 120 the correctness of our computation depends on the Generalized Riemann Hypothesis (see Section 2.4).

3 Lie algebras

The classification of the finite dimensional complex simple Lie algebras is one of the main results in modern mathematics, with a wide range of applications in such fields as group theory, geometry, and theoretical physics. Their structure and representation theory uses many combinatorial objects such as root systems, Weyl groups, weight lattices, Dynkin diagrams, etc., which makes the theory accessible for investigation by computer. For these reasons, since the 60's, many computer algebra packages and programs have been developed for dealing with various aspects of complex simple Lie algebras and their representations. As examples, we mention the package LiE [35], and the computer algebra systems MAGMA [13] and GAP4 [37], which have large libraries for computing with semisimple Lie algebras.
Also the finite dimensional real simple Lie algebras have been classified. As in the complex case, there exists a beautiful and detailed structure theory, and they are applied in various fields like differential geometry (cf. [41]) and physics (cf. [31]). However, it seems there has not been much effort yet to develop computer packages for investigating real semisimple Lie algebras by computer. An exception is the ATLAS project (cf. [30, 34]), which aims to study the unitary dual of a real Lie group.
In the next chapters I show the results about my work on Lie algebras over $\mathbb{R}$. Most of my work is done by computer, implementing well-known constructions from the literature and constructing algorithms to do so. I divided the rest of the thesis in two chapters.

The first one show my results regarding the implementation of algorithms related to simple real Lie algebras constructed from their multiplicative table.
In my joint work with Heiko Dietrich and Willem De Graaf, *"Computing with real Lie algebras: real forms, Cartan decompositions, and Cartan subalgebras"*, we developed a computer algebra package, called `CoReLG` [53] ("*Computing with Real Lie Groups*"), for working with real semisimple Lie algebras given by a multiplication table (which the ATLAS software does not do). The emphasis on representing a Lie algebra by a multiplication table allows a detailed investigation of its structure (cf. [40]). On the other hand, it also presents a range of algorithmic problems.
It is shown how to construct multiplication tables of the real semisimple Lie algebras Secondly, we show how to obtain a complete list of Cartan subalgebras or real simple Lie algebras $\mathfrak{g}$. That is a list containing exactly one elements of each G-conjugacy class of Cartan subalgebras of $\mathfrak{g}$, where G is the inner automorphism group of $\mathfrak{g}$.
The subject of the second one is the problem of finding semisimple subalgebras of real semisimple Lie algebras. The analogous problem for complex Lie algebras has been widely studied (see for example [56], [57], [62], [70]).
Let $\tilde{\mathfrak{g}}$ be a real semisimple Lie algebra with adjoint group $\widetilde{G}$. A classification of the semisimple subalgebras of $\tilde{\mathfrak{g}}$, up to $\widetilde{G}$-conjugacy, appears to be completely out of reach. Therefore we consider a weaker problem. Note that if $\mathfrak{g} \subset \tilde{\mathfrak{g}}$, then also for the complexifications, $\mathfrak{g}^c = \mathbb{C} \otimes \mathfrak{g}$, $\tilde{\mathfrak{g}}^c = \mathbb{C} \otimes \tilde{\mathfrak{g}}$ we have that $\mathfrak{g}^c \subset \tilde{\mathfrak{g}}^c$. So assume that we know an inclusion $\mathfrak{g}^c \subset \tilde{\mathfrak{g}}^c$. This leads to the following problem: let $\tilde{\mathfrak{g}}^c$ be a complex semisimple Lie algebra, and $\mathfrak{g}^c$ a complex semisimple subalgebra of it. Let $\mathfrak{g} \subset \mathfrak{g}^c$ be a real form of $\mathfrak{g}^c$. The question is **how to list, up to isomorphism, all real forms $\tilde{\mathfrak{g}} \subset \tilde{\mathfrak{g}}^c$ of $\tilde{\mathfrak{g}}^c$ such that $\mathfrak{g} \subset \tilde{\mathfrak{g}}$.**
For real semisimple Lie algebras the problem of finding and classifying the semisimple subalgebras has previously been considered in the literature. Cornwell has published a series of papers on this topic, [50], [51], [67], [68], the last two in collaboration with Ekins. Their methods require detailed case-by-case calculations, and it is not entirely

clear whether they are applicable to every subalgebra. For example, no S-subalgebras are considered in these publications (except for some S-subalgebras of type A_1 in the Lie algebras of types G_2 and F_4).
Komrakov [61] classified the maximal proper semisimple Lie subalgebras of a real simple Lie algebra. However, his paper does not give an account of the methods used. He also has a list of the real forms which contain a maximal S-subalgebra, for $\tilde{\mathfrak{g}}^c$ of exceptional type. My advisor and I find the same inclusions as Komrakov, except that in type E_6 we find a few more (see Section 5.6).
Next we turn our attention to regular semisimple subalgebras of simple real Lie algebra $\mathfrak{g}$. We give an algorithm to list the regular semisimple subalgebras of a semisimple real Lie algebra, up to conjugacy by the inner automorphism group. This uses the algorithm for listing the Cartan subalgebras of $\mathfrak{g}$, up to conjugacy. We have implemented this algorithm in the language of the computer algebra system GAP4. Using this implementation we have obtained the regular semisimple subalgebras of several real simple Lie algebras.

In the remaining of this chapter I give only preliminary results, definitions that can easily be found in the literature, that are the foundations of our work. In the first section I start by collecting some well-known facts and immediate observations concerning real forms, realifications, real structures, Killing form and Cartan subalgebras. In the second section I focus more on theory behind complex simple Lie algebras, give some other definitions about root space decomposition, root system, simple roots, Chevalley basis and canonical generators. Those are important notions that will be used later as basic step in our algorithms.

3.0.1 Comment on the notation

In my work I only deal with finite dimensional Lie algebras over the real or complex numbers. So, first of all, it is important to give some indications about the symbolic convention I use throughout this part of the thesis.

If the base field of a Lie algebra is the complex field $\mathbb{C}$, then it is emphasized by attaching a superscript "c", for example $\mathfrak{g}^c$. Lie algebras that are denoted without such a superscript have $\mathbb{R}$ as base field. If $\mathfrak{g}$ is a real simple Lie algebra, then $\mathfrak{g}^c$ denotes its complexification, so $\mathfrak{g}^c = \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$. We use the same convention for subspaces and subalgebras: if $\mathfrak{h} \subseteq \mathfrak{g}$ is a subspace, then $\mathfrak{h}^c \subseteq \mathfrak{g}^c$ denotes its complexification $\mathfrak{h}^c = \mathfrak{h} \otimes_{\mathbb{R}} \mathbb{C}$. If $\mathfrak{v}$ is a subspace of $\mathfrak{g}$ and $\mathfrak{h} \subseteq \mathfrak{g}$ a subalgebra, then $\mathfrak{z}_{\mathfrak{v}}(\mathfrak{h})$ denotes the centralizer of $\mathfrak{h}$ in $\mathfrak{v}$, that is, it is the space consisting of all $v \in \mathfrak{v}$ such that $[v, \mathfrak{h}] = 0$. If we deal with a real vector space $\mathfrak{v}$, then $\mathfrak{v}^c$ will denote its complexification, $\mathfrak{v}^c = \mathfrak{v} \otimes \mathbb{C}$. I denote the imaginary unit in $\mathbb{C}$ by $\imath$.
I use standard notation and terminology for Lie algebras, as can for instance be found in the books of Humphreys [59] and Onishchik [63]. Lie algebras will be denoted by fraktur symbols (like $\mathfrak{g}$). The adjoint representation of a Lie algebra $\mathfrak{g}$ is defined by $\mathrm{ad}_{\mathfrak{g}}\, x(y) = [x, y]$. I also just use ad if no confusion can arise about which Lie algebra is meant. Let $\mathfrak{v}$ be a subspace of the Lie algebra $\mathfrak{g}$. Then by $N_{\mathfrak{g}}(\mathfrak{v})$, $C_{\mathfrak{g}}(\mathfrak{v})$ I denote the normalizer, and centralizer of $\mathfrak{v}$ in $\mathfrak{g}$, i.e., $N_{\mathfrak{g}}(\mathfrak{v}) = \{x \in \mathfrak{g} \mid [x, \mathfrak{v}] \subset \mathfrak{v}\}$, $C_{\mathfrak{g}}(\mathfrak{v}) = \{x \in \mathfrak{g} \mid [x, \mathfrak{v}] = 0\}$.
Let $\mathfrak{g}^c$ be a complex semisimple Lie algebra, then its adjoint group, denoted G^c, is defined as the connected subgroup of $\mathrm{Aut}(\mathfrak{g}^c)$ with Lie algebra $\mathrm{ad}\, \mathfrak{g}^c$. It is the group of inner automorphisms of $\mathfrak{g}^c$; it is generated by the elements $\exp(\mathrm{ad}\, x)$ for $x \in \mathfrak{g}^c$. For

a real semisimple Lie algebra $\mathfrak{g}$ its adjoint group, denoted G, is defined as the analytic subgroup of $\mathrm{Aut}(\mathfrak{g})$, with Lie algebra $\mathrm{ad}\,\mathfrak{g}$. Also here this group is generated by the elements $\exp(\mathrm{ad}\,x)$ for $x \in \mathfrak{g}$ (see for example [41], Chapter II, §5). If $\mathfrak{g}^c = \mathbb{C} \otimes \mathfrak{g}$, then $G = G^c(\mathbb{R})$, i.e., the set of real points of G^c, or in other words, the set of $g \in G^c$ such that $g(\mathfrak{g}) = \mathfrak{g}$.
I denote the real forms of the simple Lie algebras using the convention of [60], Appendix C.3 and C.4, see also [63], Table 5.

3.0.2 Comment on the base field

In order to define a Lie algebra by a multiplication table over the reals, it usually suffices to take a subfield of the real field as base field. However, many algorithms need a Chevalley basis (see Section 3.2) at hand, which is defined over the complex field. For this reason, we require that the base field contains the imaginary unit $\imath = \sqrt{-1}$. We remark that computations with such a Chevalley basis take place behind the scenes, and the result is again defined over the reals.
In some algorithms it is necessary to take square roots of elements of the base field, so the ideal base field would contain the imaginary unit, as well as being closed under taking square roots. However, such a field is difficult to construct and to work with on a computer. As a compromise, we have provided the field $\mathbb{Q}^{\surd} = \mathbb{Q}(\{\sqrt{p} \mid p \text{ a prime}\})$; see [36, App A.1] for a comment on the implementation. We remark, however, that also over $\mathbb{Q}^{\surd}(\imath)$ a computation may fail because we cannot construct a particular square root; our observation is that this happens rather sporadically.

3.1 Real simple Lie algebras

In this section I give some basic definitions and properties regarding real Lie algebras. Most of the structures and properties are well known and can be easily be found in the literature. My first approach to the problems related to real Lie algebras was to be able to investigate many properties using a computational approach. As I said before there are not many computational tools in this field, so the first step was to implement the basis constructions for subalgebras, Cartan subalgebras real forms, etc. As first step to achieve that I list some of mathematical definition related to real Lie algebras.

Definition 14. Let $\mathfrak{g}^c$ be a complex simple (non-abelian) Lie algebra. A **real form** of $\mathfrak{g}^c$ is a real subalgebra $\mathfrak{g}$ whose complexification is isomorphic to $\mathfrak{g}^c$; in this case we can suppose that $\mathfrak{g}^c = \mathfrak{g} \oplus \imath\,\mathfrak{g}$. The **realification** $\mathfrak{g}^c(\mathbb{R})$ of $\mathfrak{g}^c$ is the Lie algebra $\mathfrak{g}^c$ considered as real.

Theorem 6. Both algebras $\mathfrak{g}$ and $\mathfrak{g}^c(\mathbb{R})$ are simple, and every real simple Lie algebra is of this kind.

Remark 3.1. I want to stress that this theorem is very important for our purpose, because it says that if we know how to implement an algorithm to construct a complex simple Lie algebras, its real forms and the the procedure of the realification we can obtain all real Lie algebras.

Definition 15. Associated with a real form $\mathfrak{g}$ is the **real structure** $\sigma\colon\ \mathfrak{g}^c \to \mathfrak{g}^c$ defined by $\sigma(a + \imath b) = a - \imath b$ for $a, b \in \mathfrak{g}$.
In this construction, the **compact real form** $\mathfrak{u}$ is of importance; this is a real form with the property that the restriction of the Killing form of $\mathfrak{g}^c$ is negative definite.

The **Killing form** of $\mathfrak{g}^c$ is the map $\kappa(x,y) = \mathrm{tr}(\mathrm{ad}\, x \circ \mathrm{ad}\, y)$ where $\mathrm{ad}\, x(z) = [x,z]$ for $x, y, z \in \mathfrak{g}^c$.

Proposition 9. The real forms of $\mathfrak{g}^c$ are, up to isomorphism, parametrized by conjugacy classes of involutive automorphisms of $\mathfrak{g}^c$, see [47, Prop 2.1].

Remark 3.2. Thanks to this proposition we see that if we can somehow characterize the involutive automorphisms of a complex simple Lie algebras we find an algorithm to do that, we can implement all real forms of it.

Since one of the basic tools I work with are Cartan subalgebras of complex semisimple Lie algebra, now I give some definitions and basic properties related to them.

Definition 16. Let $\mathfrak{g}^c$ be a semisimple Lie algebra over $\mathbb{C}$. A nilpotent subalgebra $\mathfrak{h}^c$ is said to be a Cartan subalgebra of $\mathfrak{g}^c$, if it holds:

$$L_0(\mathfrak{h}^c) := \{y \in \mathfrak{g}^c \mid \forall x \in \mathfrak{h}^c \; \exists t > 0 \text{ such that } (ad_{\mathfrak{g}^c} x)^t(y) = 0\} = \mathfrak{h}^c$$

or equivalently if $N_{\mathfrak{g}^c}(\mathfrak{h}^c)) = \mathfrak{h}^c$

There are many algorithms to construct a Cartan subalgebra. Moreover, a Lie algebra $\mathfrak{g}^c$ in general has more than one Cartan subalgebra, but in the case of algebraic closed fields it holds:

Theorem 7. Let $\mathfrak{g}^c$ be a finite dimensional Lie algebra over an algebraic closed field of characteristic 0. Let $\mathfrak{h}^c$, $\mathfrak{h}'^c$ be two Cartan subalgebras of $\mathfrak{g}^c$. then there is an element $p \in Int(\mathfrak{g}^c)$ such that $p(\mathfrak{h}^c) = \mathfrak{h}'^c$

So in the case of complex simple Lie algebra $\mathfrak{g}^c$ it is sufficient to know the group of inner automorphism of it to compute all its Cartan subalgebras. This is not the case when we work on the field of real number $\mathbb{R}$.

3.2 Constructing complex semisimple Lie algebras

The content of this section is well-known and can be found, for example, in [42, 71, 46]. Let $\mathfrak{g}^c$ be a semisimple Lie algebra over $\mathbb{C}$, with Cartan subalgebra $\mathfrak{h}^c$. Denote by $(\mathfrak{h}^c)^\star$ the dual space consisting of all linear maps $\mathfrak{h}^c \to \mathbb{C}$.

Definition 17. For $\alpha \in (\mathfrak{h}^c)^*$ set:

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g}^c \mid [h,x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}^c\}$$

and let Φ be the set of non-zero α such that $\mathfrak{g}_\alpha \neq 0$. This yields the **root space decomposition** of $\mathfrak{g}^c$

$$\mathfrak{g}^c = \mathfrak{h}^c \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

and each root space $\mathfrak{g}_\alpha$ has dimension 1.

Let $\kappa(x,y) = \mathrm{tr}(\mathrm{ad}\, x \circ \mathrm{ad}\, y)$ be the killing form of $\mathfrak{g}^c$; since κ is non-degenerate, for every $\alpha \in \Phi$ there is a unique $t_\alpha \in \mathfrak{h}^c$ with $\alpha(h) = \kappa(t_\alpha, h)$ for all $h \in \mathfrak{h}^c$. Now $(\alpha, \beta) = \kappa(t_\alpha, t_\beta) = \alpha(t_\beta)$ defines an inner product in V, the real space spanned by Φ, and Φ is a **root system** of this space.

Definition 18. A finite spanning set Φ' of a real space V with inner product $(\ ,\ )$ is a root system if the following holds:

1. if $\alpha \in \Phi'$, then $c\alpha \in \Phi'$ if and only if $c = \pm 1$;
2. Φ' is invariant under the reflection $\beta \mapsto \beta - (2(\beta,\alpha)/(\alpha,\alpha))\alpha$ for all $\alpha \in \Phi'$;
3. if $\alpha, \beta \in \Phi'$, then $2(\beta,\alpha)/(\alpha,\alpha) \in \mathbb{Z}$.

Every partial order "$<$" on V defines a set of positive elements, namely, those $v \in V$ with $0 < v$. One can choose "$<$" such that for every non-zero $\alpha \in \Phi$ either α or $-\alpha$ is positive, and such that the sum of positive elements and any positive multiple of a positive element are positive. For example, take "$<$" to be the lexicographic order defined on the coefficient vectors with respect to a fixed basis.
Such an ordering partitions Φ into positive and negative roots $\Phi = \Phi^+ \cup \Phi^-$ where $\Phi^- = -\Phi^+$. The corresponding **basis of simple roots** $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ consists of those $\alpha \in \Phi^+$ which cannot be written as $\alpha = \beta + \gamma$ with $\beta, \gamma \in \Phi^+$. The set Δ is a basis of V and every $\alpha \in \Phi$ is an integral linear combination of elements in Δ with either all coefficients non-negative or all coefficients non-positive. For $\alpha, \beta \in V$ define:

$$\langle \alpha, \beta^\vee \rangle = 2(\alpha,\beta)/(\beta,\beta);$$

this expression is linear only in the first component.
Consider the converse situation and start with an abstract root system Φ in an ℓ-dimensional Euclidean space V with inner product $(\ ,\ )$. Let $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ be a basis of simple roots, and consider the associated multiplication table (4.1) on abstract elements $h_1, \ldots, h_\ell$ and x_α with $\alpha \in \Phi$. If the signs of the $N_{\alpha,\beta}$ have been chosen such that this multiplication table satisfies the Jacobi identity, then we have constructed a complex semisimple Lie algebra with root system Φ. This approach to constructing complex semisimple Lie algebras from root systems was first proposed by Tits [48], cf. [42, Notes p. 151]. However, his method for determining the signs does not immediately lead to an algorithm. Later, algorithmic methods for determining the signs appeared, see for example [33, 40, 44, 49].

3.2.1 Chevalley basis

Let $\mathfrak{g}^c$ be a semisimple Lie algebra over $\mathbb{C}$. Let $\mathfrak{h}^c$ be a fixed Cartan subalgebra of $\mathfrak{g}^c$, and let Φ denote the corresponding root system. By $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ we denote a basis of simple roots of Φ, corresponding to a choice of positive roots Φ^+. For $\alpha, \beta \in \Phi$ we let r, q be the maximal integers such that $\beta - r\alpha$ and $\beta + q\alpha$ lie in Φ, and we define $\langle \beta, \alpha^\vee \rangle = r - q$. For $\alpha \in \Phi$ we denote by $\mathfrak{g}^c_\alpha$ the corresponding root space in $\mathfrak{g}^c$.

Proposition 10. There is a basis of $\mathfrak{g}^c$ formed by elements $h_1, \ldots, h_\ell \in \mathfrak{h}^c$, along with $x_\alpha \in \mathfrak{g}^c_\alpha$ for $\alpha \in \Phi$ such that:

$$\begin{aligned}
[h_i, h_j] &= 0 \\
[h_i, x_\alpha] &= \langle \alpha, \alpha_i^\vee \rangle x_\alpha \\
[x_\alpha, x_{-\alpha}] &= h_\alpha \\
[x_\alpha, x_\beta] &= N_{\alpha,\beta} x_{\alpha+\beta},
\end{aligned}$$

where h_α is the unique element in $[\mathfrak{g}^c_\alpha, \mathfrak{g}^c_{-\alpha}]$ with $[h_\alpha, x_\alpha] = 2x_\alpha$.

For convenience, when we refer to a multiplication table of this form, we define $N_{\alpha,\beta} = 0$ and $x_{\alpha+\beta} = 0$ whenever $\alpha, \beta \in \Phi$ with $\alpha + \beta \notin \Phi \cup \{0\}$.
This implies that $h_{\alpha_i} = h_i$ for $1 \leq i \leq \ell$. Furthermore, $N_{\alpha,\beta} = \pm(r+1)$, where r is the maximal integer with $\alpha - r\beta \in \Phi$. Also we define $x_\gamma = 0$ if $\gamma \notin \Phi$.
A basis with these properties is called a **Chevalley basis** of $\mathfrak{g}^c$ (see [59], §25.2).

3.2.2 Canonical generators

For $1 \leq i \leq \ell$ let g_i, x_i, y_i be elements of $\mathfrak{g}^c$ such that

$$\begin{aligned} [g_i, g_j] &= 0 \\ [g_i, x_j] &= \langle \alpha_j, \alpha_i^\vee \rangle x_j \\ [g_i, y_j] &= -\langle \alpha_j, \alpha_i^\vee \rangle y_j \\ [x_i, y_j] &= \delta_{ij} g_i. \end{aligned} \tag{3.1}$$

A set of 3ℓ elements with these commutation relations is called a **canonical generating set** of $\mathfrak{g}^c$ ([71], §IV.3).

Proposition 11. We have the following:

- A canonical generating set of $\mathfrak{g}^c$ generates $\mathfrak{g}^c$.
- Sending one canonical generating set to another one uniquely extends to an automorphism of $\mathfrak{g}^c$.

Let $\mathfrak{h}^c$ be a Cartan subalgebra with basis $h_1, \ldots, h_l$ with associate root system Φ. An example of a canonical generating set is the following: $g_i = h_i$, $x_i = x_{\alpha_i}$, $y_i = x_{-\alpha_i}$, where $\alpha \in \Phi$ is a positive root.

4 Real Forms

The aim of this chapter is to describe an efficient construction of the realification and the real forms of $\mathfrak{g}^c$ by computer, the results of my joint work with Heiko Dietrich and Willem De Graaf, *"Computing with real Lie algebras: real forms, Cartan decompositions, and Cartan subalgebras"*.
In a computer algebra system, a Lie algebra is usually represented by a structure constants table with respect to a chosen basis. Using the known classification of the automorphisms of $\mathfrak{g}^c$, it is a technical exercise to write down bases for all real forms of $\mathfrak{g}^c$ up to isomorphism, see [36, §2] for a recent description. Computing the structure constants table from such a basis in the conventional way requires $n(n-1)/2$ multiplications in $\mathfrak{g}^c$, where $\mathfrak{g}^c$ has dimension n, and for each multiplication $O(n^2)$ additions are necessary to write the product as a linear combination of the basis elements; this yields an algorithm which needs $O(n^4)$ algebra operations. Here we describe an alternative. Namely, we determine the structure constants of a real form theoretically, which allows us to write down the structure constants table directly, leading to an algorithm which needs $O(n^2)$ algebra operations. Moreover, for each real form (and the realification), our analysis allows us to write down explicitly a basis of a Cartan subalgebra which splits over the Gaussian rationals. For this Cartan subalgebra we can readily compute the corresponding root system, and a Chevalley basis. The real simple Lie algebras we construct come with all this information;

We proceed as follows. In Section one I explain our algorithmic results, in the second section I show how to construct of the compact form $\mathfrak{u}$ of a real Lie algebras given a complex simple Lie algebra $\mathfrak{g}^c$ and one of its Cartan subalgebras $\mathfrak{h}^c$ with root system Φ. Here the main ingredient is the Chevalley basis associate to $\mathfrak{h}^c$ and Φ. We give directly the multiplication table of $\mathfrak{u}$ with respect to a chosen basis.
In section three I explain how to construct all non compact real form starting from the compact one. This is done by classifying all involutive automorphism associate to $\mathfrak{g}^c$. This can conveniently be done using KAC diagrams associated to $\mathfrak{g}^c$. We give directly the multiplication table of those real forms with respect to a chosen basis. In section four I show the construction of the realifications of $\mathfrak{g}^c$. Section five contains some definitions concerning Cartan decomposition of a real form of $\mathfrak{g}$ of $\mathfrak{g}^c$. Classification of strongly orthogonal root systems are the key to achieve these results. In the last section I show some example of runtimes of our algorithms.

4.1 Main results

Let $\mathfrak{g}^c$ be a complex simple Lie algebra; let $\mathfrak{g}$ be a real semisimple Lie algebra with adjoint group G. In my joint work with Heiko Dietrich and the professor De Graaf Willem, *"Computing with real Lie algebras: real forms, Cartan decompositions, and Cartan subalgebras"* we describe algorithms for the following two tasks:

(a) Up to isomorphism, construct all real forms of $\mathfrak{g}^c$;
(b) Up to G-conjugacy, construct all Cartan subalgebras of $\mathfrak{g}$;

More details and precise definitions are given in the corresponding sections.

Our approach for (a) is to exploit the known theoretical classification of real forms of $\mathfrak{g}^c$ (which in turn requires the classification of involutive automorphisms of $\mathfrak{g}^c$); we construct these real forms by writing down explicitly a structure constants table with respect to some basis. Our implementation of (b) is a constructive version of a classification theorem due to Sugiura [73].

4.1.1 Comment on Cartan subalgebras

There exist efficient algorithms to construct a Cartan subalgebra of a Lie algebra given by a multiplication table, cf. [39, 40]. However, we do remark that the computation of the associated root system may fail because the program does not succeed in splitting the Cartan subalgebra over the base field (or an extension thereof of small degree). The problem of finding Cartan subalgebras which can be split is very difficult, cf. [43]. Therefore, if in our algorithms we have to construct a Cartan subalgebra, we assume that it has a small splitting field. Constructing the corresponding root system can then be done with linear algebra methods.

4.2 Constructing the compact form

In this section I describe the construction of the compact form $\mathfrak{u}$ of the complex simple Lie algebra $\mathfrak{g}^c$.
Let $\mathfrak{g}^c$ be a complex simple Lie algebra and $\mathfrak{h}^c$ a Carta subalgebra; as said before there exists a **Chevalley basis**, $\{h_1, \ldots, h_\ell, x_\alpha \mid \alpha \in \Phi\}$ of $\mathfrak{g}^c$, where $\{h_1, \ldots, h_\ell\}$ is a basis of $\mathfrak{h}^c$, each $x_\alpha \in \mathfrak{g}_\alpha$, and the following commutation relations are satisfied; let $\alpha, \beta \in \Phi$ and $i, j \in \{1, \ldots, \ell\}$:

$$[h_i, h_j] = 0, \quad [h_i, x_\alpha] = \langle \alpha, \alpha_i^\vee \rangle x_\alpha, \quad [x_\alpha, x_{-\alpha}] = h_\alpha, \tag{4.1}$$
$$[x_\alpha, x_\beta] = N_{\alpha,\beta} x_{\alpha+\beta} \quad \text{if } \alpha + \beta \in \Phi, \text{ and} \quad [x_\alpha, x_\beta] = 0 \quad \text{if } \alpha + \beta \notin \Phi \cup \{0\}.$$

On these relations we remark the following. First,

$$|N_{\alpha,\beta}| = r + 1 \quad \text{and} \quad N_{\alpha,\beta} = -N_{-\alpha,-\beta},$$

where $r \geq 0$ is the largest integer such that $\beta - r\alpha \in \Phi$. Second, $h_i = h_{\alpha_i}$, and

$$h_\alpha = \sum\nolimits_{i=1}^{\ell} n_i^\alpha h_i$$

where n_i^α is defined by $\alpha^\vee = \sum_{i=1}^{\ell} n_i^\alpha \alpha_i^\vee$; recall that $\Phi^\vee = \{\alpha^\vee \mid \alpha \in \Phi\}$ with $\alpha^\vee = (2/(\alpha, \alpha))\alpha$ is a root system with basis of simple roots $\{\alpha_1^\vee, \ldots, \alpha_\ell^\vee\}$; thus, if $\alpha \in \Phi$, then $n_1^\alpha, \ldots, n_\ell^\alpha$ are integers and either all non-negative, or all non-positive.

Remark 4.1. Except from the signs of the $N_{\alpha,\beta}$, all coefficients in the multiplication table (4.1) are determined completely by the root system and choice of simple roots.

Let $\mathfrak{g}^c$ be a complex simple Lie algebra with multiplication table (4.1) defined with respect to a Chevalley basis $\{h_1, \ldots, h_\ell, x_\alpha \mid \alpha \in \Phi\}$.

Proposition 12. The compact real form $\mathfrak{u}$ of $\mathfrak{g}^c$ is unique up to conjugacy [47].

For $\alpha \in \Phi$ define:

$$H_\alpha = \imath h_\alpha, \quad X_\alpha = x_\alpha - x_{-\alpha}, \quad Y_\alpha = \imath(x_\alpha + x_{-\alpha}).$$

Since $X_{-\alpha} = -X_\alpha$ and $Y_{-\alpha} = Y_\alpha$, these elements are not linearly independent; however,

$$\mathcal{B}_\mathfrak{u} = \{H_\alpha, X_\beta, Y_\beta \mid \alpha \in \Delta,\ \beta \in \Phi^+\}$$

is linearly independent. If $\mathfrak{u} = \mathrm{Span}_\mathbb{R}(\mathcal{B}_\mathfrak{u})$ is the $\mathbb{R}$-span of the elements in $\mathcal{B}_\mathfrak{u}$, then $\mathfrak{u}$ is closed under taking Lie brackets and $\mathfrak{g}^c = \mathfrak{u} \oplus \imath\,\mathfrak{u}$, hence $\mathfrak{u}$ is a real form of $\mathfrak{g}^c$. It follows from the proof of [46, Thm 6.11] that $\mathfrak{u}$ is compact; the associated real structure $\tau\colon\ \mathfrak{g}^c \to \mathfrak{g}^c$ satisfies

$$\tau(h_\alpha) = -h_\alpha \quad \text{and} \quad \tau(x_\alpha) = -x_{-\alpha}.$$

If $\alpha - \beta \in \Phi^-$ then $X_{\alpha-\beta} = -X_{\beta-\alpha}$ with $X_{\beta-\alpha} \in \mathcal{B}_\mathfrak{u}$ and $Y_{\alpha-\beta} = Y_{\beta-\alpha} \in \mathcal{B}_\mathfrak{u}$. Using (4.1), one can determine the following multiplication table of $\mathfrak{u}$ with respect to $\mathcal{B}_\mathfrak{u}$; let $\alpha, \beta \in \Phi$ with $\alpha \neq \beta$:

$$\begin{array}{rclrcl}
[H_\alpha, H_\beta] &=& 0, & [H_\alpha, X_\beta] &=& \langle\beta, \alpha^\vee\rangle Y_\beta, \\
[X_\alpha, X_\beta] &=& N_{\alpha,\beta}X_{\alpha+\beta} - N_{\alpha,-\beta}X_{\alpha-\beta}, & [H_\alpha, Y_\beta] &=& -\langle\beta, \alpha^\vee\rangle X_\beta, \\
[X_\alpha, Y_\beta] &=& N_{\alpha,\beta}Y_{\alpha+\beta} + N_{\alpha,-\beta}Y_{\alpha-\beta}, & [H_\alpha, X_\alpha] &=& 2Y_\alpha, \\
[Y_\alpha, Y_\beta] &=& -N_{\alpha,\beta}X_{\alpha+\beta} - N_{\alpha,-\beta}X_{\alpha-\beta}, & [H_\alpha, Y_\alpha] &=& -2X_\alpha, \\
[X_\alpha, Y_\alpha] &=& 2H_\alpha. & & &
\end{array} \tag{4.2}$$

The corresponding structure constants table has integral entries only. The subspace of $\mathfrak{u}$ spanned by $\{H_{\alpha_1}, \ldots, H_{\alpha_\ell}\}$ has dimension ℓ and is a Cartan subalgebra of $\mathfrak{u}$. Using (4.2), it is straightforward to write down the associated root system. Similarly, we can express the given Chevalley basis $\{h_1, \ldots, h_\ell, x_\alpha \mid \alpha \in \Phi\}$ as $\mathbb{Q}(\imath)$-linear combinations of the basis elements $\mathcal{B}_\mathfrak{u}$.

$$x_\alpha = \tfrac{1}{2}(X_\alpha - iY_\alpha) \qquad x_{-\alpha} = -\tfrac{1}{2}(X_\alpha + iY_\alpha) \qquad h_\alpha = -iH_\alpha \tag{4.3}$$

4.3 Constructing non-compact real forms

We retain the notation of the previous section and show how to construct the non-compact real forms of $\mathfrak{g}^c$ from the compact form $\mathfrak{u}$. For this purpose, let θ be an involutive automorphism of $\mathfrak{g}^c$, commuting with the real structure τ. Then θ leaves $\mathfrak{u}$ invariant and we have a decomposition $\mathfrak{u} = \mathfrak{u}_+ \oplus \mathfrak{u}_-$ of $\mathfrak{u}$ into the ±1-eigenspaces of θ. Setting $\mathfrak{k} = \mathfrak{u}_+$ and $\mathfrak{p} = \imath\,\mathfrak{u}_-$, we get that

$$\mathfrak{g} = \mathfrak{g}(\mathfrak{u}, \theta) = \mathfrak{k} \oplus \mathfrak{p}$$

is a real form of $\mathfrak{g}^c$ whose associated real structure is $\sigma = \tau \circ \theta = \theta \circ \tau$.
Conversely, every real form of $\mathfrak{g}^c$ is isomorphic to $\mathfrak{g}(\mathfrak{u}, \theta)$ for some involutive automorphism θ commuting with τ, and, moreover, $\mathfrak{g}(\mathfrak{u}, \theta)$ and $\mathfrak{g}(\mathfrak{u}, \theta')$ are isomorphic if and only if θ and θ' are conjugate in $\mathrm{Aut}(\mathfrak{g}^c)$, see [47, Prop 2.1 and Thm 3.2]. By running over all involutions θ (up to conjugacy) commuting with τ, one can construct all real forms of $\mathfrak{g}^c$ up to isomorphism.

4.3.1 Kac diagrams

The finite order automorphisms of $\mathfrak{g}^c$ are, up to conjugacy, classified by so-called Kac diagrams, see [38, §3.3.7] or [41, §X.5]. It follows that, up to conjugacy, an involutive automorphism of $\mathfrak{g}^c$ can be given by two pieces of data. The first is an involutive permutation π of $\{1,\dots,\ell\}$ such that $\langle \alpha_{\pi(i)}, \alpha_{\pi(j)}^\vee\rangle = \langle \alpha_i, \alpha_j^\vee\rangle$ for all $i,j \in \{1,\dots,\ell\}$; in [47] this is called an automorphism of Δ. This permutation π induces a map (denoted by the same symbol) $\pi\colon \Phi \to \Phi$ defined by $\pi(\sum_{i=1}^\ell m_i\alpha_i) = \sum_{i=1}^\ell m_i\alpha_{\pi(i)}$; this is an automorphism of the root system Φ. The second piece of data is a list $(\varepsilon_1,\dots,\varepsilon_\ell)$ with $\varepsilon_i \in \{1,-1\}$ and $\varepsilon_i = \varepsilon_{\pi(i)}$ for all i. It follows from [47, (II.22)] that the map defined by $x_{\pm\alpha_i} \mapsto \varepsilon_i x_{\pm\alpha_{\pi(i)}}$ and $h_i \mapsto h_{\pi(i)}$ extends to an involutive automorphism θ of $\mathfrak{g}^c$. By definition, if $\alpha \in \Phi$, then

$$\theta\colon \begin{cases} h_\alpha & \mapsto h_{\pi(\alpha)} \\ x_\alpha & \mapsto \varepsilon_\alpha x_{\pi(\alpha)}, \end{cases}$$

where each $\varepsilon_\alpha \in \{\pm 1\}$ such that for all $\alpha,\beta \in \Phi$ we have

$$\varepsilon_\alpha = \varepsilon_{-\alpha} = \varepsilon_{\pi(\alpha)} \quad \text{and} \quad N_{\alpha,\beta}\varepsilon_{\alpha+\beta} = N_{\pi(\alpha),\pi(\beta)}\varepsilon_\alpha\varepsilon_\beta.$$

We remark that every involutive automorphism of $\mathfrak{g}^c$ is conjugate to an automorphism of this form. Moreover, the Kac diagram of an involution of $\mathfrak{g}^c$ immediately yields the data required for the above construction, that is, π and $(\varepsilon_1,\dots,\varepsilon_\ell)$.

4.3.2 Constructing the multiplication table

We now reconsider the form $\mathfrak{g} = \mathfrak{g}(\mathfrak{u},\theta) = \mathfrak{k} \oplus \mathfrak{p}$ with θ as above. Using the basis $\mathcal{B}_u$ of $\mathfrak{u}$ with multiplication table (4.2), we define for $\alpha \in \Phi$:

$$\begin{aligned} \overline{H}_\alpha^0 &= H_\alpha + H_{\pi(\alpha)}, & \overline{H}_\alpha^1 &= \imath(H_\alpha - H_{\pi(\alpha)}), \\ \overline{X}_\alpha^0 &= X_\alpha + \varepsilon_\alpha X_{\pi(\alpha)}, & \overline{X}_\alpha^1 &= \imath(X_\alpha - \varepsilon_\alpha X_{\pi(\alpha)}), \\ \overline{Y}_\alpha^0 &= Y_\alpha + \varepsilon_\alpha Y_{\pi(\alpha)}, & \overline{Y}_\alpha^1 &= \imath(Y_\alpha - \varepsilon_\alpha Y_{\pi(\alpha)}). \end{aligned}$$

Note that $\overline{X}_{\pi(\alpha)}^0 = \varepsilon_\alpha \overline{X}_\alpha^0$ and $\overline{X}_{-\alpha}^0 = -\overline{X}_\alpha^0$; moreover, $\overline{X}_\alpha^0 = 0$ if and only if $\alpha = \pi(\alpha)$ and $\varepsilon_\alpha = -1$. Similar relations hold for $\overline{H}_\alpha^i$, $\overline{X}_\alpha^i$, and $\overline{Y}_\alpha^i$ with $i \in \{0,1\}$. It follows readily that

$$\mathfrak{k} = \mathrm{Span}_{\mathbb{R}}(\{\overline{H}_\alpha^0, \overline{X}_\alpha^0, \overline{Y}_\alpha^0 \mid \alpha \in \Phi\}) \quad \text{and} \quad \mathfrak{p} = \mathrm{Span}_{\mathbb{R}}(\{\overline{H}_\alpha^1, \overline{X}_\alpha^1, \overline{Y}_\alpha^1 \mid \alpha \in \Phi\}).$$

In the following, we use the convention that the upper indices are considered modulo 2, that is, $\overline{H}_\alpha^2 = \overline{H}_\alpha^0$, and so on. Using (4.2), we get the following relations; let $\alpha,\beta \in \Phi$:

$$\begin{aligned} [\overline{H}_\alpha^i, \overline{H}_\beta^j] &= 0, \\ [\overline{H}_\alpha^i, \overline{X}_\beta^j] &= (-1)^{ij}\langle \beta + (-1)^i\pi(\beta), \alpha^\vee\rangle \overline{Y}_\beta^{i+j}, \\ [\overline{H}_\alpha^i, \overline{Y}_\beta^j] &= -(-1)^{ij}\langle \beta + (-1)^i\pi(\beta), \alpha^\vee\rangle \overline{X}_\beta^{i+j}, \\ [\overline{X}_\alpha^i, \overline{X}_\beta^j] &\overset{\alpha\neq\beta}{=} (-1)^{ij}N_{\alpha,\beta}\overline{X}_{\alpha+\beta}^{i+j} - (-1)^{ij}N_{\alpha,-\beta}\overline{X}_{\alpha-\beta}^{i+j} + (-1)^{(i+1)j}\varepsilon_\beta N_{\alpha,\pi(\beta)}\overline{X}_{\alpha+\pi(\beta)}^{i+j} - \\ &\qquad (-1)^{(i+1)j}\varepsilon_\beta N_{\alpha,-\pi(\beta)}\overline{X}_{\alpha-\pi(\beta)}^{i+j}, \end{aligned}$$

$$
\begin{aligned}
[\overline{X}^0_\alpha, \overline{X}^1_\alpha] &= -\varepsilon_\alpha N_{\alpha,\pi(\alpha)} \overline{X}^1_{\alpha+\pi(\alpha)}, \\
[\overline{X}^i_\alpha, \overline{Y}^j_\beta] &\overset{\alpha\neq\beta}{=} (-1)^{ij} N_{\alpha,\beta} \overline{Y}^{i+j}_{\alpha+\beta} + (-1)^{ij} N_{\alpha,-\beta} \overline{Y}^{i+j}_{\alpha-\beta} + (-1)^{(i+1)j} \varepsilon_\beta N_{\alpha,\pi(\beta)} \overline{Y}^{i+j}_{\alpha+\pi(\beta)} + \\
&\quad (-1)^{(i+1)j} \varepsilon_\beta N_{\alpha,-\pi(\beta)} \overline{Y}^{i+j}_{\alpha-\pi(\beta)}, \\
[\overline{X}^i_\alpha, \overline{Y}^j_\alpha] &= (-1)^{ij} 2\overline{H}^{i+j}_\alpha + (-1)^j (1-(-1)^{i+j}) \varepsilon_\alpha N_{\alpha,\pi(\alpha)} \overline{Y}^{i+j}_{\alpha+\pi(\alpha)}, \\
[\overline{Y}^i_\alpha, \overline{Y}^j_\beta] &\overset{\alpha\neq\beta}{=} -(-1)^{ij} N_{\alpha,\beta} \overline{X}^{i+j}_{\alpha+\beta} - (-1)^{ij} N_{\alpha,-\beta} \overline{X}^{i+j}_{\alpha-\beta} - (-1)^{(i+1)j} \varepsilon_\beta N_{\alpha,\pi(\beta)} \overline{X}^{i+j}_{\alpha+\pi(\beta)} - \\
&\quad (-1)^{(i+1)j} \varepsilon_\beta N_{\alpha,-\pi(\beta)} \overline{X}^{i+j}_{\alpha-\pi(\beta)}, \\
[\overline{Y}^0_\alpha, \overline{Y}^1_\alpha] &= \varepsilon_\alpha N_{\alpha,\pi(\alpha)} \overline{X}^1_{\alpha+\pi(\alpha)}.
\end{aligned}
$$

In order to get a multiplication table of $\mathfrak{g}$, we first select a subset $\mathcal{B}_\mathfrak{g}$ of the above elements that forms a basis of $\mathfrak{g}$. This can be done, for instance, by extending the root order "$<$" to a total order on Φ, and defining $\mathcal{B}_\mathfrak{g}$ as the union of the sets

$$
\begin{aligned}
&\{\overline{H}^0_\alpha \mid \alpha \in \Delta,\ \alpha = \pi(\alpha)\}, \\
&\{\overline{H}^i_\alpha \mid \alpha \in \Delta,\ \alpha < \pi(\alpha),\ i \in \{0,1\}\}, \\
&\{\overline{X}^i_\alpha, \overline{Y}^i_\alpha \mid \alpha \in \Phi^+,\ \pi(\alpha) = \alpha,\ \varepsilon_\alpha = (-1)^i,\ i \in \{0,1\}\}, \\
&\{\overline{X}^i_\alpha, \overline{Y}^i_\alpha \mid \alpha \in \Phi^+,\ \alpha < \pi(\alpha),\ i \in \{0,1\}\}.
\end{aligned}
$$

Subsequently, the multiplication table of $\mathfrak{g}$ with respect to $\mathcal{B}_\mathfrak{g}$ can be worked out using the above commutation relations; this is mainly a question of good book-keeping, and does not present any theoretical difficulties. With respect to this basis, the multiplication table only has integral entries.

Proposition 13. A subalgebra of $\mathfrak{g}$ is a Cartan subalgebra if and only if its complexification is a Cartan subalgebra of $\mathfrak{g}^c$.

Thus the set of all $\overline{H}^i_\alpha$ with $\alpha \in \Phi$ and $i \in \{0,1\}$ spans a Cartan subalgebra of $\mathfrak{g}$, whereas the set of all $\overline{H}^0_\alpha$ with $\alpha \in \Phi$ spans a Cartan subalgebra of $\mathfrak{k}$. Since this Cartan subalgebra of $\mathfrak{g}$ splits over $\mathbb{Q}(\imath)$, it is easy to compute the corresponding root system. Again, the original Chevalley basis can be written as $\mathbb{Q}(\imath)$-linear combinations of elements in $\mathcal{B}_\mathfrak{g}$.

If $\pi(\alpha) = \alpha$, then $h_\alpha = -\frac{i}{2}\overline{H}^0_\alpha$
If $\pi(\alpha) = \alpha$ and $\varepsilon_\alpha = -1$, then $x_\alpha = -\frac{1}{4}i(\overline{X}^1_\alpha - i\overline{Y}^1_\alpha)$ and $x_{-\alpha} = \frac{1}{4}i(\overline{X}^1_\alpha + i\overline{Y}^1_\alpha)$.
If $\pi(\alpha) = \alpha$ and $\varepsilon_\alpha = 1$, then $x_\alpha = -\frac{1}{4}(\overline{X}^0_\alpha - i\overline{Y}^0_\alpha)$ and $x_{-\alpha} = \frac{1}{4}(\overline{X}^0_\alpha + i\overline{Y}^0_\alpha)$.
If $\pi(\alpha) > \alpha$, then:

- $x_\alpha = \frac{1}{2\varepsilon_\alpha}[\overline{X}^0_\alpha - i\overline{X}^1_\alpha - i(\overline{Y}^0_\alpha - i\overline{Y}^1_\alpha)]$
- $x_{-\alpha} = -\frac{1}{2\varepsilon_\alpha}[\overline{X}^0_\alpha - i\overline{X}^1_\alpha + i(\overline{Y}^0_\alpha - i\overline{Y}^1_\alpha)]$
- $x_{\pi(\alpha)} = \frac{1}{2\varepsilon_\alpha}[\overline{X}^0_\alpha + i\overline{X}^1_\alpha - i(\overline{Y}^0_\alpha + i\overline{Y}^1_\alpha)]$
- $x_{\pi(-\alpha)} = -\frac{1}{2\varepsilon_\alpha}[\overline{X}^0_\alpha + i\overline{X}^1_\alpha + i(\overline{Y}^0_\alpha + i\overline{Y}^1_\alpha)]$

4.4 Constructing the realification

In this section I show how to construct the realification of a complex simple (non-abelian) Lie algebra $\mathfrak{g}^c$ with a Cartan subalgebra $\mathfrak{h}^c \subseteq \mathfrak{g}^c$, corresponding root system Φ, and Chevalley basis $\{h_1 \ldots, h_\ell, x_\alpha \mid \alpha \in \Phi\}$. Clearly, the realification $\mathfrak{g}^c(\mathbb{R})$ of $\mathfrak{g}^c$ satisfies $\dim_{\mathbb{R}} \mathfrak{g}^c(\mathbb{R}) = 2 \dim_{\mathbb{C}} \mathfrak{g}^c$ and has a basis

$$\mathcal{B} = \{h_1^\varepsilon, \ldots, h_\ell^\varepsilon, x_\alpha^\varepsilon \mid \alpha \in \Phi,\ \varepsilon \in \{0,1\}\}$$

where $h_i^\varepsilon = h_i$ and $x_\alpha^\varepsilon = x_\alpha$ if $\varepsilon = 0$, and $h_i^\varepsilon = \imath h_i$ and $x_\alpha^\varepsilon = \imath x_\alpha$ if $\varepsilon = 1$. Similarly, we define $h_\alpha^0 = h_\alpha$ and $h_\alpha^1 = \imath h_\alpha$ for $\alpha \in \Phi$. Again, the upper labels are read modulo 2, for example, $h_i^2 = h_i^0$. The structure constants of $\mathfrak{g}^c(\mathbb{R})$ with respect to $\mathcal{B}$ are as follows; let $a, b \in \{0,1\}$:

$$\begin{aligned}
[h_\alpha^a, h_\beta^b] &= 0, \\
[h_\alpha^a, x_\beta^b] &= (-1)^{ab} \langle \beta, \alpha^\vee \rangle x_\beta^{a+b}, \\
[x_\alpha^a, x_\beta^b] &\overset{\alpha+\beta \neq 0}{=} (-1)^{ab} N_{\alpha,\beta} x_{\alpha+\beta}^{a+b}, \\
[x_\alpha^a, x_{-\alpha}^b] &= (-1)^{ab} h_\alpha^{a+b}.
\end{aligned}$$

Let $\tau \colon \mathfrak{g}^c \to \mathfrak{g}^c$ be the compact real structure defined in Section 4.2; recall that $\tau(h_\alpha) = -h_\alpha$ and $\tau(x_\alpha) = -x_{-\alpha}$ for all $\alpha \in \Phi$. As shown in [47, Ex 2.4], the map $(x, y) \mapsto (\tau(y), \tau(x))$ is a real structure of the complex Lie algebra $\mathfrak{g}^c \oplus \mathfrak{g}^c$, with associated real form

$$\hat{\mathfrak{g}} = \{(x, \tau(x)) \mid x \in \mathfrak{g}^c\} \subseteq \mathfrak{g}^c \oplus \mathfrak{g}^c$$

Moreover, it is shown that $\varphi \colon \hat{\mathfrak{g}} \to \mathfrak{g}^c(\mathbb{R})$, $(x, \tau(x)) \mapsto x$, is an isomorphism. Using φ, one can readily verify that

$$\mathfrak{h} = \mathrm{Span}_{\mathbb{R}}(\{h_1^\varepsilon, \ldots, h_\ell^\varepsilon \mid \varepsilon \in \{0,1\}\}) \subseteq \mathfrak{g}^c(\mathbb{R})$$

is a Cartan subalgebra of $\mathfrak{g}^c(\mathbb{R})$. We now construct a Chevalley basis of $\mathfrak{g}^c(\mathbb{R})$; for $\alpha \in \Phi$ define

$$\begin{aligned}
u_\alpha^0 &= \tfrac{1}{2}(x_\alpha^0 + \imath x_\alpha^1), & u_\alpha^1 &= \tfrac{1}{2}(x_\alpha^0 - \imath x_\alpha^1), \\
k_\alpha^0 &= \tfrac{1}{2}(h_\alpha^0 + \imath h_\alpha^1), & k_\alpha^1 &= \tfrac{1}{2}(h_\alpha^0 - \imath h_\alpha^1),
\end{aligned}$$

and write $k_i^\varepsilon = k_{\alpha_i}^\varepsilon$ for $i \in \{1, \ldots, \ell\}$. We claim that

$$\{k_1^0, k_1^1, \ldots, k_\ell^0, k_\ell^1, u_\alpha^0, u_\alpha^1 \mid \alpha \in \Phi\}$$

is a Chevalley basis of $\mathfrak{g}^c(\mathbb{R})$. To prove this, let $\mathfrak{a}_i = \mathrm{Span}_{\mathbb{C}}(\{k_1^i, \ldots, k_\ell^i, u_\alpha^i \mid \alpha \in \Phi\})$ for $i \in \{0,1\}$. A direct computation shows that each $\mathfrak{a}_i$ is an ideal of the complexification of $\mathfrak{g}^c(\mathbb{R})$, that is, of $\mathfrak{g}^c \oplus \mathfrak{g}^c$. Moreover, $[\mathfrak{a}_1, \mathfrak{a}_2] = 0$, thus $\mathfrak{g}^c \oplus \mathfrak{g}^c = \mathfrak{a}_1 \oplus \mathfrak{a}_2$. The structure constants table of each $\mathfrak{a}_i$ (with respect to the defining basis) is the same as the structure constants table of $\mathfrak{g}^c$ (with respect to its Chevalley basis); this implies the assertion. Note that $\mathfrak{h} = \mathrm{Span}_{\mathbb{R}}(\{k_\alpha^j \mid j \in \{0,1\},\ \alpha \in \Phi\})$, which splits over $\mathbb{Q}(\imath)$, and it is straightforward to compute the associated root system.

4.5 Cartan subalgebras

Let $\mathfrak{g}^c$ be a complex semisimple Lie algebra with a real form $\mathfrak{g}$.

Definition 19. A **Cartan decomposition** of $\mathfrak{g}$ is a decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ with:

$$(1)\ [\mathfrak{k},\mathfrak{k}], [\mathfrak{p},\mathfrak{p}] \subseteq \mathfrak{k} \qquad (2)\ [\mathfrak{p},\mathfrak{p}] \subseteq \mathfrak{k} \qquad (3)\ [\mathfrak{p},\mathfrak{k}] \subseteq \mathfrak{p}$$

such that its associated **Cartan involution** $\theta\colon\ \mathfrak{g} \to \mathfrak{g}$ defined by $\theta(k+p) = k - p$ for $k \in \mathfrak{k}$ and $p \in \mathfrak{p}$ induces a positive definite form $\kappa_\theta(x,y) = -\kappa(x,\theta(y))$ on $\mathfrak{g}$, see [47, §5]; here κ is the Killing form of $\mathfrak{g}^c$.

Cartan decompositions are unique up to conjugation by inner automorphisms of $\mathfrak{g}$.The next lemma shows that we already know Cartan decompositions for the real simple Lie algebras constructed in the last sections.

Lemma 4. a) With the notation of the Sections 4.2 and 4.3, a Cartan decomposition of $\mathfrak{g} = \mathfrak{g}(\mathfrak{u},\theta)$ is $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$; the associated Cartan involution is $\theta|_{\mathfrak{g}}$.
b) With the notation of Section 4.4, $\mathfrak{g}^c(\mathbb{R}) = \mathfrak{k} \oplus \mathfrak{p}$ is a Cartan decomposition, where

$$\begin{aligned} \mathfrak{k} &= \mathrm{Span}_{\mathbb{R}}(\{h_1^1, \ldots, h_\ell^1, x_\alpha^0 - x_{-\alpha}^0, x_\alpha^1 + x_{-\alpha}^1 \mid \alpha \in \Phi\}), \\ \mathfrak{p} &= \mathrm{Span}_{\mathbb{R}}(\{h_1^0, \ldots, h_\ell^0, x_\alpha^1 - x_{-\alpha}^1, x_\alpha^0 + x_{-\alpha}^0 \mid \alpha \in \Phi\}). \end{aligned}$$

Proof. Part a) follows from [47, §5]. Part b) follows from [47, Ex 3.4], which shows that $\hat{\mathfrak{g}} \to \hat{\mathfrak{g}}$, $(x, \tau(x)) \mapsto (\tau(x), x)$, is a Cartan involution of $\hat{\mathfrak{g}}$ (with $\hat{\mathfrak{g}}$ as defined in Section 4.4). □

Here $\mathfrak{g}^c$ is a complex semisimple Lie algebra, and $\mathfrak{g}$ is a real form with Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$. Denote by G^c and G the adjoint group of $\mathfrak{g}^c$ and $\mathfrak{g}$, respectively. It is well-known that all Cartan subalgebras of $\mathfrak{g}^c$ are conjugate under G^c, whereas, in general, the Cartan subalgebras of $\mathfrak{g}$ are not conjugate under G. Following a theorem of Sugiura [73], we now address the construction of all Cartan subalgebras of $\mathfrak{g}$ up to G-conjugacy.

To describe this construction, we first have to introduce the notion of Cartan subspaces and strongly orthogonal sets of roots, see Sections 4.5.1 and 4.5.2; in Section 4.5.3 we state Sugiura's classification. The results of this section also apply to the realification $\mathfrak{g}^c(\mathbb{R})$, which is a real form of $\mathfrak{g}^c \oplus \mathfrak{g}^c$. We note that Kostant [45] obtain a classification theorem similar to that of Sugiura.

4.5.1 Constructing Cartan subspaces

Definition 20. A **Cartan subspace** of $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ is defined to be a maximal abelian subspace of $\mathfrak{p}$.

Cartan subspaces exist and are unique up to conjugacy. The following algorithm computes a basis of a Cartan subspace of $\mathfrak{p}$.

Algorithm 1
Here $\mathfrak{g}$ is a real semisimple Lie algebra with Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$; the output C is a basis of a Cartan subspace of $\mathfrak{g}$

1. Set $C = \emptyset$, $\mathfrak{c} = \{0\}$, and $Z = \mathfrak{p}$
2. While { not $Z = \mathfrak{c}$ } do:
3. choose $c \in Z \setminus \mathfrak{c}$ and define $C := C \cup \{c\}$
4. construct $\mathfrak{c} = \mathrm{Span}_{\mathbb{R}}(C)$ and $Z = \mathfrak{z}_{\mathfrak{p}}(\mathfrak{c}) := \{x \in \mathfrak{p} \mid [x, c] = 0 \; \forall c \in \mathfrak{c}\}$
5. end.
6. Return C;

4.5.2 Constructing strongly orthogonal sets of roots

Here we consider an abstract root system Ψ in an Euclidean space V with inner product $(\ ,\ )$. A subset $\beta = \{\beta_1, \ldots, \beta_s\}$ of Ψ is **strongly orthogonal** if $\beta_i \neq \pm\beta_j$ and $\beta_i \pm \beta_j \notin \Psi$ for all $i \neq j$. Clearly, the image of β under an element of the Weyl group W of Ψ is also strongly orthogonal. We will need a classification of the strongly orthogonal subsets of Ψ up to W-conjugacy – which is known in the literature, see [73] – and an efficient algorithm for deciding whether two given strongly orthogonal sets are W-conjugate; note that running over all elements of W is not efficient in general. For each type of irreducible root system, we now give a classification of its strongly orthogonal subsets, together with a method for deciding W-conjugacy.
We use the well-known constructions of the root systems of type B_n, C_n, and D_n, and their Weyl groups, see for example [32]. For the other types, we express each root as linear combination of the simple roots; for this we use the ordering of simple roots as defined in [32]. The correctness of the given classifications can be verified directly for root systems of classical type; for the exceptional types, we have used a computer program to double-check the results.
If Ψ has basis of simple roots $\{\alpha_1, \ldots, \alpha_n\}$, then we denote the set of associated fundamental weights by $\{\lambda_1, \ldots, \lambda_n\}$; recall that these are defined by the conditions $2(\lambda_i, \alpha_j)/(\alpha_j, \alpha_j) = \delta_{ij}$ with $i, j \in \{1, \ldots, n\}$, see [46, App C.1]. If $X \subseteq V$ is a W-stable subset and $\Gamma \subseteq \Psi$, then we define

$$\Gamma_X = X \cap \mathrm{Span}_{\mathbb{Q}}(\Gamma);$$

note that the cardinality of Γ_X is the same for all W-conjugates of Γ.
Recall that either all roots in Ψ have the same length, or there exist exactly two root lengths; in the latter case, there is a natural partition into **short** and **long roots**, see [42, §10.4]. We now list, up to W-conjugacy, the strongly orthogonal subsets of an irreducible root system Ψ. We make a case distinction on the type of Ψ; the notation in each case is independent from the other cases.

Type A_n:
Here $\Psi = \pm\{\alpha_i + \alpha_{i+1} + \cdots + \alpha_j \mid 1 \le i \le j \le n\}$, and, up to W-conjugacy, the strongly orthogonal sets are $\Gamma_k = \{\alpha_1, \alpha_3, \ldots, \alpha_k\}$ where k runs over the odd integers between 1 and n. Note that the W-class of a strongly orthogonal set is determined by the cardinality of the set.

Type B_n:
Let V be spanned by $\{v_1, \ldots, v_n\}$ with inner product defined by $(v_i, v_j) = \delta_{ij}$. The root system of type B_n can be defined as $\Psi = \{\pm v_i \pm v_j \mid i < j\} \cup \{\pm v_i \mid 1 \le i \le j\}$. The corresponding Weyl group is $W = U \rtimes S_n$, where the symmetric group S_n acts on V by $\sigma \cdot v_i = v_{\sigma(i)}$, the abelian (multiplicative) group $U = \{u = (u_1, \ldots, u_n) \mid u_i = \pm 1\}$ acts on V by $u \cdot v_i = u_i v_i$, and S_n acts on U by permuting the entries of u. For odd integers k, l with $-1 \le k \le l \le n$, we define

$$\Gamma_{k,l} = \{v_1 - v_2, v_3 - v_4, \ldots, v_l - v_{l+1}\} \cup \{v_1 + v_2, v_3 + v_4, \ldots, v_k + v_{k+1}\}.$$

Up to W-conjugacy, the strongly orthogonal sets are $\Gamma_{k,l}$, where k, l are odd integers with $-1 \le k \le l \le n$, along with $\Gamma_{k',l'} \cup \{v_n\}$, where k', l' are odd integers with $-1 \le k' \le l' \le n-2$. Note that $v_1 = \lambda_1$, and define $X = \{\pm v_i \mid 1 \le i \le n\}$; observe that X is the W-orbit of v_1. We have $|(\Gamma_{k,l})| = (l+k)/2 + 1$, $|(\Gamma_{k,l})_X| = 2k + 2$, $|\Gamma_{k',l'} \cup \{v_n\}| = (l' + k')/2 + 2$, $|(\Gamma_{k',l'} \cup \{v_n\})_X| = 2k' + 4$. So if Γ is a strongly orthogonal set, then by computing $|\Gamma|$, $|\Gamma_X|$, and the number of long roots in Γ, we can determine to which of the above sets Γ is conjugate to.

Type C_n:
Here V and W are the same as for B_n, but $\Psi = \{\pm v_i \pm v_j \mid i < j\} \cup \{\pm 2v_i \mid 1 \le i \le j\}$. Up to W-conjugacy, the strongly orthogonal sets are

$$\Gamma_{k,l} = \{v_1 - v_2, v_3 - v_4, \ldots, v_k - v_{k+1}, 2v_{k+1}, \ldots, 2v_l\},$$

where k, l are integers with $-1 \le k < l \le n$ and k odd. Now $|\Gamma_{k,l}| = l - (k+1)/2$, and $\Gamma_{k,l}$ has exactly $(k+1)/2$ short roots. The size and the number of short roots determine the W-class of a strongly orthogonal subset uniquely.

Type D_n:
The space V is as for B_n and C_n, but here we have $\Psi = \{\pm v_i \pm v_j \mid i < j\}$. The Weyl group is $W = \widetilde{U} \rtimes S_n$ where $\widetilde{U} = \{u \in U \mid \prod_i u_i = 1\}$ with U as in case B_n. Up to W-conjugacy, the strongly orthogonal sets are

$$\Gamma_{k,l} = \{v_1 - v_2, v_3 - v_4, \ldots, v_l - v_{l+1}\} \cup \{v_1 + v_2, v_3 + v_4, \ldots, v_k + v_{k+1}\},$$

where k, l are odd integers with $-1 \le k \le l \le n$; note that $|\Gamma_{k,l}| = (k+l)/2 + 1$. If n is even, then there is another strongly orthogonal set, namely,

$$\Gamma_0 = \{v_1 - v_2, v_3 - v_4, \ldots, v_{n-3} - v_{n-2}, v_{n-1} + v_n\}.$$

Define $X = \{\pm v_i \mid 1 \le i \le n\}$ as for type B_n; note that X is W-stable and $|(\Gamma_{k,l})_X| = 2k + 2$. This cardinality does not distinguish the sets $\Gamma_{-1,n-1}$ and Γ_0 if $n = 2m$ is even. In that case we set $v = v_1 + \cdots + v_n$ and

$$Y = W \cdot v = \left\{ \sum\nolimits_{i=1}^{n} a_i v_i \mid a_i = \pm 1 \text{ and } a_1 \cdots a_n = 1 \right\}.$$

Clearly, Y is W-invariant. If m is even, then $|(\Gamma_0)_Y| = 0$ and $|(\Gamma_{-1,n-1})_Y| = 2^m$; if m is odd then $|(\Gamma_0)_Y| = 2^m$ and $|(\Gamma_{-1,n-1})_Y| = 0$. Note that X is the W-orbit of the fundamental weight λ_1, whereas Y is the W-orbit of $2\lambda_n$.

Type E_6:
Up to W-conjugacy, the strongly orthogonal sets in this case are $\{\alpha_1\}$, $\{\alpha_1, \alpha_2\}$, $\{\alpha_1, \alpha_2, \alpha_5\}$, and $\{\alpha_1, \alpha_2, \alpha_5, \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5\}$.

Type E_7:
Let $\beta = \alpha_1 + 2\alpha_2 + 2\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7$. Up to W-conjugacy, the strongly orthogonal sets are $\Gamma_1 = \{\alpha_1\}$, $\Gamma_2 = \{\alpha_1, \alpha_2\}$, $\Gamma_{3,1} = \{\alpha_1, \alpha_2, \alpha_5\}$, $\Gamma_{3,2} = \Gamma_2 \cup \{\beta\}$, $\Gamma_{4,1} = \Gamma_{3,1} \cup \{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5\}$, $\Gamma_{4,2} = \Gamma_{3,1} \cup \{\alpha_7\}$, $\Gamma_5 = \Gamma_{4,1} \cup \{\alpha_7\}$, $\Gamma_6 = \Gamma_5 \cup \{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + 2\alpha_5 + 2\alpha_6 + \alpha_7\}$, and $\Gamma_7 = \Gamma_6 \cup \{\beta\}$. Sets of the same cardinality can be distinguished as follows: if $X = W \cdot \lambda_7$ (a set of size 56) and $d \in \{3, 4\}$, then $|(\Gamma_{d,1})_X| = 0$, whereas $|(\Gamma_{d,2})_X| = 8$.

Type E_8:
Let $\gamma = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 2\alpha_7 + \alpha_8$. Up to W-conjugacy, the strongly orthogonal sets are $\Gamma_1 = \{\alpha_1\}$, $\Gamma_2 = \{\alpha_1, \alpha_2\}$, $\Gamma_3 = \Gamma_2 \cup \{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5\}$, $\Gamma_{4,1} = \Gamma_3 \cup \{\alpha_8\}$, $\Gamma_{4,2} = \Gamma_3 \cup \{\gamma\}$, $\Gamma_5 = \Gamma_{4,1} \cup \{\alpha_5\}$, $\Gamma_6 = \Gamma_5 \cup \{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + 2\alpha_5 + 2\alpha_6 + 2\alpha_7 + \alpha_8\}$, $\Gamma_7 = \Gamma_6 \cup \{\alpha_1 + 2\alpha_2 + 2\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + 2\alpha_7 + \alpha_8\}$, and $\Gamma_8 = \Gamma_7 \cup \{\gamma\}$. The two sets of the same cardinality can be distinguished as follows: if $X = \Psi$, then $|(\Gamma_{4,1})_X| = 8$, whereas $|(\Gamma_{4,2})_X| = 24$.

Type F_4:
Up to W-conjugacy, the strongly orthogonal sets are $\Gamma_{1,1} = \{\alpha_3\}$, $\Gamma_{1,2} = \{\alpha_1\}$, $\Gamma_{2,1} = \Gamma_{1,1} \cup \{\alpha_2 + 2\alpha_3 + 2\alpha_4\}$, $\Gamma_{2,2} = \Gamma_{1,2} \cup \{\alpha_1 + 2\alpha_2 + 2\alpha_3\}$, $\Gamma_{3,1} = \Gamma_{2,1} \cup \{2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4\}$, $\Gamma_{3,2} = \Gamma_{2,2} \cup \{\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4\}$, and $\Gamma_4 = \Gamma_{3,2} \cup \{\alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4\}$. Sets of the same cardinality have different numbers of long roots.

Type G_2:
Up to W-conjugacy, the strongly orthogonal sets are $\{\alpha_1\}$, $\{\alpha_2\}$, and $\{\alpha_1, 3\alpha_2 + 2\alpha_2\}$; note that α_1 and α_2 have different lengths.

We summarize the obtained criterion on non-conjugacy in the following proposition.

Proposition 14. Let Ψ be an irreducible root system with Weyl group W. Let $\Gamma, \Gamma' \subseteq \Psi$ be strongly orthogonal sets. Depending on the type of Ψ, the sets Γ and Γ' are not W-conjugate if and only if

• Type A_n, C_n, E_6, F_4, or G_2: $|\Gamma| \neq |\Gamma'|$, or Γ, Γ' have a different number of long roots.

• Type B_n: $|\Gamma| \neq |\Gamma'|$, or $|\Gamma_X| \neq |\Gamma'_X|$ with $X = W \cdot \lambda_1$, or Γ and Γ' have a different number of long roots.

• Type D_n: $|\Gamma| \neq |\Gamma'|$, or $|\Gamma_X| \neq |\Gamma'_X|$ with $X = W \cdot \lambda_1$, or $|\Gamma_Y| \neq |\Gamma'_Y|$ with $Y = W \cdot 2\lambda_n$.

• Type E_7: $|\Gamma| \neq |\Gamma'|$, or $|\Gamma_X| \neq |\Gamma'_X|$ with $X = W \cdot \lambda_7$.

• Type E_8: $|\Gamma| \neq |\Gamma'|$, or $|\Gamma_X| \neq |\Gamma'_X|$ with $X = \Psi$.

The last condition for type D_n is only needed if $n = 2m$ and $|\Gamma| = |\Gamma'| = m$.

4.5.3 Constructing Cartan subalgebras

Proposition 15. Let $\mathfrak{c} \subseteq \mathfrak{p}$ be a fixed Cartan subspace of $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$, and let $\mathfrak{h}_0^+$ be a Cartan subalgebra of the centralizer $\mathfrak{z}_{\mathfrak{k}}(\mathfrak{c})$. Than $\mathfrak{h}_0 = \mathfrak{h}_0^+ \oplus \mathfrak{c}$ is a Cartan subalgebra of $\mathfrak{g}$, thus its complexification $\mathfrak{h}_0^c$ is a Cartan subalgebra of $\mathfrak{g}^c$.

Let Φ be the root system of $\mathfrak{g}^c$ with respect to $\mathfrak{h}_0^c$, with Chevalley basis $\{h_1, \ldots, h_\ell, x_\alpha \mid \alpha \in \Phi\}$. The Killing form κ is non-degenerate on $\mathfrak{h}_0$, and therefore also on $\mathfrak{h}_0^+$ and $\mathfrak{c}$. Now let $\Phi_{\mathfrak{c}}$ be the set consisting of roots $\alpha \in \Phi$ such that $h_\alpha = [x_\alpha, x_{-\alpha}]$ lies in $\mathfrak{c}$; observe that this is a subroot system of Φ. The following theorem is due to Sugiura [73]; it implies the correctness of Algorithm 2.

Theorem 8 (Sugiura)**.** Let $\mathfrak{c} \subseteq \mathfrak{p}$ be a fixed Cartan subspace of $\mathfrak{g}$; let Φ and $\Phi_{\mathfrak{c}}$ be defined as above, and let W be the Weyl group of Φ. Denote by A the set of G-conjugacy classes of Cartan subalgebras of $\mathfrak{g}$. Let B be the set of W-conjugacy classes of strongly orthogonal subsets of $\Phi_{\mathfrak{c}}$. For a representative $\Gamma = \{\beta_1, \ldots, \beta_s\}$ of a W-class in B let $\mathfrak{l}_\Gamma = \mathrm{Span}_{\mathbb{R}}(\{h_{\beta_1}, \ldots, h_{\beta_s}\})$, and define $\mathfrak{h}_\Gamma = \mathfrak{h}_\Gamma^+ \oplus \mathfrak{h}_\Gamma^-$ where

$\mathfrak{h}_\Gamma^- = \{x \in \mathfrak{c} \mid \kappa(x, y) = 0 \text{ for all } y \in \mathfrak{l}_\Gamma\}$, and

$\mathfrak{h}_\Gamma^+$ a Cartan subalgebra of $\mathfrak{z}_{\mathfrak{k}}(\mathfrak{h}_\Gamma^-)$.

Then $\mathfrak{h}_\Gamma$ is a Cartan subalgebra of $\mathfrak{g}$, and $\Gamma^W \to (\mathfrak{h}_\Gamma)^G$ is a bijection $A \to B$.

Algorithm 2
Here $\mathfrak{g}$ is a real simple Lie algebra with adjoint group G; the output is a list of Cartan subalgebras of $\mathfrak{g}$ up to conjugacy under G

- Compute a Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$, and a Cartan subspace $\mathfrak{c} \subseteq \mathfrak{p}$
- Set $\mathfrak{h}_0 = \mathfrak{h}_0^+ \oplus \mathfrak{c}$ where $\mathfrak{h}_0^+$ be a Cartan subalgebra of $\mathfrak{z}_{\mathfrak{k}}(\mathfrak{c})$
- Compute the root system Φ of $\mathfrak{g}^c$ with respect to $\mathfrak{h}_0^c$, and a Chevalley basis $\{h_1, \ldots, h_\ell, x_\alpha \mid \alpha \in \Phi\}$
- Let Ψ be the set of $\alpha \in \Phi$ such that $h_\alpha = [x_\alpha, x_{-\alpha}] \in \mathfrak{c}$
- Compute the set B of strongly orthogonal subsets of Ψ
- from B remove W-conjugate copies, where W is the Weyl group of Φ
- Let $\mathcal{H}$ be the set consisting of $\mathfrak{h}_\Gamma$, defined as in Theorem 8, where Γ runs over B
- Return $\mathcal{H}$

4.6 Implementation and runtimes

The algorithms described in this chapter (and some other methods) are implemented for the computer algebra system GAP4 [37], as part of the package `CoReLG` [53]. The following examples were computed on a computer with Intel(R) Core(TM) i7-3770 CPU 3.40GHz and 16GM RAM. The next table shows the running time in seconds for the construction of a multiplicative table (Table) of several real semisimple Lie algebras, and their Cartan subalgebras (CSA). We work over the field $\mathbb{Q}(i)$, which in GAP is connoted by the command $CF(4)$. I show also the same results working on the square root field, which in GAP is connoted by the command $SqrtField$,

Algebra	Table $CF(4)$	CSA $CF(4)$	Table $SqrtField$	CSA $SqrtField$
$\mathfrak{su}_6$	0.016	0.016	0.036	0.112
$\mathfrak{su}_{1,5}$	0.012	0.096	0.044	0.628
$\mathfrak{su}_{2,4}$	0.016	0.112	0.040	0.652
$\mathfrak{su}_{3,3}$	0.012	0.124	0-040	0.060
$\mathfrak{sl}_3(\mathcal{H})$	0.008	0.112	0.048	0.560
$\mathfrak{sl}_6(\mathbb{R})$	0.012	0.152	0.048	0.556
$\mathfrak{su}_{11}$	0.093	0.176	0.288	1.972
$\mathfrak{su}_{1,10}$	0.140	1.040	3.188	8.580
$\mathfrak{su}_{2,9}$	0.136	3.828	0.356	11.153
$\mathfrak{su}_{3,8}$	0.136	3.828	0.364	8.325
$\mathfrak{su}_{4,7}$	0.136	1.040	0.360	11.181
$\mathfrak{su}_{5,6}$	0.140	1.092	0.360	11.265
$\mathfrak{sl}_{11}(\mathbb{R})$	0.136	1.228	0.420	11.224
$\mathfrak{su}_{21}$	2.541	3.632	7.008	105.127
$\mathfrak{su}_{1,20}$	4.748	52.379	7.188	483.947
$\mathfrak{su}_{2,19}$	5.037	69.076	7.781	587.960
$\mathfrak{su}_{3,18}$	4.768	40.555	9.629	485.558
$\mathfrak{su}_{4,17}$	4.704	36.310	7.213	489.362

Table 4: Runtimes for the type A_n for $n = 5, 10, 20$

Algebra	Table $CF(4)$	CSA $CF(4)$	Table $SqrtField$	CSA $SqrtField$
$\mathfrak{so}_{11}$	0.036	0.044	0.072	0.240
$\mathfrak{so}_{2,9}$	0.036	0.312	0.092	1.324
$\mathfrak{so}_{4,7}$	0.020	0.324	0.088	1.436
$\mathfrak{so}_{6,5}$	0.032	0.348	0.068	1.312
$\mathfrak{so}_{8,3}$	0.028	0.264	0.076	1.496
$\mathfrak{so}_{10,1}$	0.024	0.204	0.092	1.348
$\mathfrak{so}_{21}$	0.368	0.624	0.812	15.013
$\mathfrak{so}_{2,19}$	0.584	4.781	1.100	49.075
$\mathfrak{so}_{4,17}$	0.576	5.152	1.108	46.495
$\mathfrak{so}_{6,15}$	0.588	9.393	1.128	49.975
$\mathfrak{so}_{8,13}$	0.576	9.197	1.096	53.979
$\mathfrak{so}_{10,11}$	0.584	8.297	1.100	68.244
$\mathfrak{so}_{12,9}$	0.580	7.604	1.100	64.564
$\mathfrak{so}_{14,7}$	0.573	6.208	1.100	55.607
$\mathfrak{so}_{16,5}$	0.689	9.048	1.128	51.263
$\mathfrak{so}_{18,3}$	3.677	4.604	1.104	44.255
$\mathfrak{so}_{20,1}$	0.604	8.228	1.108	50.683
$\mathfrak{so}_{41}$	14.697	27.162	25.618	793.945
$\mathfrak{so}_{2,39}$	36.355	339.305	41.654	3241.819

Table 5: Runtimes for the type B_n for $n = 5, 10, 20$

Algebra	Table $CF(4)$	CSA $CF(4)$	Table $SqrtField$	CSA $SqrtField$
$\mathfrak{sp}_5$	0.036	0.052	0.076	0.296
$\mathfrak{sp}_{1,4}$	0.028	0.236	0.092	1.328
$\mathfrak{sp}_{2,3}$	0.036	0.244	0.100	1.288
$\mathfrak{sp}_5(\mathbb{R})$	0.032	0.264	0.092	1.400
$\mathfrak{sp}_{10}$	0.608	0.792	1.020	15.561
$\mathfrak{sp}_{1,9}$	0.812	4.700	1.325	47.879
$\mathfrak{sp}_{2,8}$	0.800	7.020	1.320	44.611
$\mathfrak{sp}_{3,7}$	0.824	4.944	1.348	50.992
$\mathfrak{sp}_{4,6}$	0.816	8.704	1.500	48.195
$\mathfrak{sp}_{5,5}$	0.808	5.001	1.348	51.967
$\mathfrak{sp}_{10}(\mathbb{R})$	0.912	8.873	1.340	64.232
$\mathfrak{sp}_{20}$	25.597	38.407	33.126	735.374
$\mathfrak{sp}_{1,19}$	55.559	441.050	54.891	3203.353

Table 6: Runtimes for the type C_n for $n = 5, 10, 20$

Algebra	Table $CF(4)$	CSA $CF(4)$	Table $SqrtField$	CSA $SqrtField$
$\mathfrak{so}_{10}$	0.020	0.032	0.052	0.172
$\mathfrak{so}_{2,8}$	0.020	0.184	0.064	0.944
$\mathfrak{so}_{4,6}$	0.024	0.220	0.056	0.992
$\mathfrak{so}^*(10)$	0.016	0.204	0.056	1.044
$\mathfrak{so}_{9,1}$	0.020	0.160	0.068	0.864
$\mathfrak{so}_{3,7}$	0.012	0.180	0.064	0.916
$\mathfrak{so}_{5,5}$	0.016	0.244	0.068	0.984
$\mathfrak{so}_{20}$	0.248	0.444	0.652	9.465
$\mathfrak{so}_{2,18}$	0.428	7.260	0.892	38.475
$\mathfrak{so}_{4,16}$	0.432	3.796	0.904	40.263
$\mathfrak{so}_{6,14}$	0.436	8.840	0.884	39.163
$\mathfrak{so}_{8,12}$	0.432	5.232	0.900	47.279
$\mathfrak{so}_{10,10}$	0.428	5.404	0.905	45.834
$\mathfrak{so}^*(20)$	0.420	3.485	0.860	37.114
$\mathfrak{so}19,1$	0.424	2.744	1.048	36.495
$\mathfrak{so}_{3,17}$	0.416	6.880	1.032	44.263
$\mathfrak{so}_{5,15}$	0.512	5.680	1.008	55.668
$\mathfrak{so}_{7,13}$	0.420	4.436	0.920	42.339
$\mathfrak{so}_{9,11}$	0.440	9.036	0.928	43.763
$\mathfrak{so}_{40}$	17.013	26.830	20.813	678.419
$\mathfrak{so}_{2,38}$	27.886	338.409	39.602	2585.338

Table 7: Runtimes for the type D_n for $n = 5, 10, 20$

Algebra	Table $CF(4)$	CSA $CF(4)$	Table $SqrtField$	CSA $SqrtField$
E_6^{cmp}	0.052	0.088	0.128	0.648
EI	0.056	0.584	0.200	3.036
EII	0.048	0.500	0.164	2.876
$EIII$	0.064	0.448	0.144	7.357
EIV	0.060	0.404	0.180	2.528
E_7^{cmp}	0.120	0.228	0.324	2.648
EV	0.168	1.588	0.452	19.602
EVI	0.188	1.556	0.408	13.753
$EVII$	0.196	1.424	0.408	13.769
E_7^{cmp}	0.484	0.844	1.148	22.429
$EVIII$	1.012	14.009	1.896	80.917
EIX	0.852	7.237	6.028	74.949

Table 8: Runtimes for the type E_6, E_7 and E_8

Algebra	Table $CF(4)$	CSA $CF(4)$	Table $SqrtField$	CSA $SqrtField$
F_4^{cmp}	0.028	0.044	0.104	0.384
$F_4(4)$	0.028	0.392	0.108	2.048
$F_4(-20)$	0.036	0.240	0.084	1.368
G_2^{cmp}	0.008	0.008	0.008	0.024
$G_2(2)$	0.004	0.044	0.008	0.032

Table 9: Runtimes for the type F_4 and G_2

5 Semisimple Subalgebras

The subject of this part of my thesis is the problem of finding semisimple subalgebras of real semisimple Lie algebras. The analogous problem for complex Lie algebras has been widely studied (see for example [56], [57], [62], [70]). In order to describe the main results in this area I need to introduce some terminology. Let $\tilde{\mathfrak{g}}^c$ be a semisimple complex Lie algebra, with adjoint group $\widetilde{G}^c$ (this is the group of inner automorphisms).

Definition 21. Two complex subalgebras $\mathfrak{g}_1^c, \mathfrak{g}_2^c \subset \tilde{\mathfrak{g}}^c$ are said to be **equivalent** if there is an $\eta \in \widetilde{G}^c$ with $\eta(\mathfrak{g}_1^c) = \mathfrak{g}_2^c$. They are called **linearly equivalent** if for all representations $\rho : \tilde{\mathfrak{g}}^c \to \mathfrak{gl}(V^c)$ we have that the subalgebras $\rho(\mathfrak{g}_1^c)$, $\rho(\mathfrak{g}_2^c)$ are conjugate under $\mathrm{GL}(V^c)$.

Definition 22. A subalgebra of $\tilde{\mathfrak{g}}^c$ is called **regular** if it is normalized by a Cartan subalgebra of $\tilde{\mathfrak{g}}^c$. An S-subalgebra is a subalgebra not contained in a regular subalgebra.

We have the following:

- There is an algorithm to determine the regular semisimple subalgebras of $\tilde{\mathfrak{g}}^c$, up to equivalence [57].
- The maximal semisimple S-subalgebras of the simple Lie algebras of classical type [56], and the semisimple S-subalgebras of the simple Lie algebras of exceptional type [57] have been classified up to equivalence.
- The simple subalgebras of the Lie algebras of exceptional type have been classified up to equivalence [62].
- The semisimple subalgebras of the simple Lie algebras of ranks not exceeding 8 have been classified up to linear equivalence [70].

Now let $\tilde{\mathfrak{g}}$ be a real semisimple Lie algebra with adjoint group $\widetilde{G}$. A classification of the semisimple subalgebras of $\tilde{\mathfrak{g}}$, up to $\widetilde{G}$-conjugacy, appears to be completely out of reach. Therefore my advisor and I consider a weaker problem. Note that if $\mathfrak{g} \subset \tilde{\mathfrak{g}}$, then also for the complexifications, $\mathfrak{g}^c = \mathbb{C} \otimes \mathfrak{g}$, $\tilde{\mathfrak{g}}^c = \mathbb{C} \otimes \tilde{\mathfrak{g}}$ we have that $\mathfrak{g}^c \subset \tilde{\mathfrak{g}}^c$. So assume that we know an inclusion $\mathfrak{g}^c \subset \tilde{\mathfrak{g}}^c$. This leads to the following problem: let $\tilde{\mathfrak{g}}^c$ be a complex semisimple Lie algebra, and $\mathfrak{g}^c$ a complex semisimple subalgebra of it. Let $\mathfrak{g} \subset \mathfrak{g}^c$ be a real form of $\mathfrak{g}^c$. List, up to isomorphism, all real forms $\tilde{\mathfrak{g}} \subset \tilde{\mathfrak{g}}^c$ of $\tilde{\mathfrak{g}}^c$ such that $\mathfrak{g} \subset \tilde{\mathfrak{g}}$.
I recall the following fact:

Proposition 16. Let $\tilde{\mathfrak{g}}, \tilde{\mathfrak{g}}' \subset \tilde{\mathfrak{g}}^c$ be two real forms of $\tilde{\mathfrak{g}}^c$. Then $\tilde{\mathfrak{g}}$ and $\tilde{\mathfrak{g}}'$ are isomorphic if and only if there is a $\phi \in \mathrm{Aut}(\tilde{\mathfrak{g}}^c)$ such that $\phi(\tilde{\mathfrak{g}}) = \tilde{\mathfrak{g}}'$.

Because of this we can reformulate the problem as follows: let $\varepsilon : \mathfrak{g}^c \hookrightarrow \tilde{\mathfrak{g}}^c$ be an embedding of complex semisimple Lie algebras. Let $\mathfrak{g} \subset \mathfrak{g}^c$ be a real form. List, up to isomorphism, all real forms $\tilde{\mathfrak{g}}$ of $\tilde{\mathfrak{g}}^c$ such that there is a $\phi \in \mathrm{Aut}(\tilde{\mathfrak{g}}^c)$ with $\phi(\varepsilon(\mathfrak{g})) \subset \tilde{\mathfrak{g}}$. That is the main problem of this part of the thesis.

Let $\tilde{\mathfrak{g}}_1, \ldots, \tilde{\mathfrak{g}}_m$ be the non-compact real forms of $\tilde{\mathfrak{g}}^c$ (i.e., each non-compact real form of $\tilde{\mathfrak{g}}^c$ is isomorphic to exactly one $\tilde{\mathfrak{g}}_i$). In our setting the $\tilde{\mathfrak{g}}_i$ are given by a basis and a multiplication table. We describe algorithmic methods that help to solve the following problem: given an embedding $\varepsilon : \mathfrak{g}^c \hookrightarrow \tilde{\mathfrak{g}}^c$, and a real form $\mathfrak{g}$ of $\mathfrak{g}^c$, find all i such that there is an automorphism ϕ of $\tilde{\mathfrak{g}}^c$ such that $\phi(\varepsilon(\mathfrak{g})) \subset \tilde{\mathfrak{g}}_i$, along with a basis of the subalgebra $\phi(\varepsilon(\mathfrak{g}))$ of $\tilde{\mathfrak{g}}_i$ in terms of a basis of $\tilde{\mathfrak{g}}_i$. Our algorithms reduce this problem to finding the solution to a set of polynomial equations. We show some nontrivial examples where it is possible to deal with these polynomial equations. The approach proposed here is particularly well suited for S-subalgebras; at the end of the chapter I give a list of all $\tilde{\mathfrak{g}}_i$, when $\tilde{\mathfrak{g}}^c$ is of exceptional type and the image of ε is an S-subalgebra of $\tilde{\mathfrak{g}}^c$.

Now I give an outline of the chapter. The next section contains concepts and constructions from the literature that we use. I also give an algorithm to compute equivalences of representations of semisimple Lie algebras, which may not have been described before, but follows immediately from the representation theory of such algebras. In Sections 5.2, 5.3 and 5.4 we describe our method. Section 5.5 has some examples computed using our implementation. Finally, in Section 5.6 we give the list of real semisimple subalgebras of the real simple Lie algebras of exceptional type, that correspond to S-subalgebras of the corresponding complex simple Lie algebras. From Section 5.7, the main problem is to classify the semisimple subalgebras up to the action by the inner automorphism group. In Section 5.8 I recall some other definition on Cartan subalgebras such as compact dimension and give the algorithm for finding generators of $W(\mathfrak{h})$ the real Weyl group of a θ-stable $\mathfrak{h}$ Cartan subalgebra of g. In Section 5.9 I give a brief description a Dynkin algorithm to list the semisimple subalgebras of a complex semisimple Lie algebra $\mathfrak{g}^c$, up to conjugacy by the adjoint group G^c . In Section 5.10 I give algorithms to checks whether a given $\mathfrak{h}$-regular semisimple subalgebra is strongly $\mathfrak{h}$-regular and for giving a list of strongly $\mathfrak{h}$-regular semisimple subalgebras of g, such that each such subalgebra of g is G-conjugate to exactly one element of the list. Finally in Section 5.11 I give the list list of strongly $\mathfrak{h}$-regular semisimple subalgebras of some algebras $\mathfrak{g}$.

5.1 Computing endomorphism spaces

Here $\mathfrak{g}^c$ is a complex semisimple Lie algebra with canonical generators h_i, x_i, y_i for $1 \leq i \leq \ell$. Let $\mathfrak{h}^c$ denote the span of the h_i (a Cartan subalgebra of $\mathfrak{g}^c$). First we review some of the basic facts of the representation theory of $\mathfrak{g}^c$ (see [59], §20).

Definition 23. Let $\rho : \mathfrak{g}^c \to \mathfrak{gl}(V^c)$ be a finite-dimensional representation of $\mathfrak{g}^c$. For $\mu \in (\mathfrak{h}^c)^*$ we set $V^c_\mu = \{v \in V^c \mid \rho(h)v = \mu(h)v\}$. If $V^c_\mu \neq 0$ then μ is called a **weight** of ρ (or of the $\mathfrak{g}^c$-module V^c), and V^c_μ is the corresponding **weight space**. Elements of V^c_μ are called weight vectors of weight μ.

Proposition 17. V^c is the sum of its weight spaces.

Definition 24. Let $v \in V^c_\mu$ and suppose that $\rho(x_i)v = 0$ for $1 \leq i \leq \ell$. Then v is called a **highest weight vector**, and μ a **highest weight** of ρ.

Proposition 18. Suppose that ρ is irreducible. Then there is a unique highest weight λ. Moreover, $\dim V^c_\lambda = 1$. Let $v_\lambda \neq 0$ be a highest weight vector of weight λ. Then there is a set S_λ of sequences $(i_1, \ldots, i_k)$, with $k \geq 0$ and $1 \leq i_r \leq \ell$ such that the elements $\rho(y_{i_1}) \cdots \rho(y_{i_k})v_\lambda$ form a basis of V^c.

Remark 5.1. S_λ is not uniquely determined. But for each λ we fix one S_λ.

Now let $\varphi : \mathfrak{g}^c \to \mathfrak{gl}(W^c)$ be another irreducible representation of $\mathfrak{g}^c$ with the same highest weight λ. Let $w_\lambda \neq 0$ be a highest weight vector of weight λ. Define the linear map $A : V^c \to W^c$ that maps $\rho(y_{i_1}) \cdots \rho(y_{i_k})v_\lambda$ to $\varphi(y_{i_1}) \cdots \varphi(y_{i_k})w_\lambda$, for all $(i_1, \ldots, i_k) \in S_\lambda$.

Lemma 5.2. *We have $A\rho(x) = \varphi(x)A$ for all $x \in \mathfrak{g}^c$.*

Proof. Since ρ, φ are irreducible representations of $\mathfrak{g}^c$ with the same highest weight, there exists an isomorphism, that is, a bijective linear map $A' : V^c \to W^c$ with $A'\rho(x)v = \varphi(x)A'v$ for all $x \in \mathfrak{g}^c$ and $v \in V^c$. This implies that $A'v_\lambda = aw_\lambda$ where $a \in \mathbb{C}$, $a \neq 0$. It also follows that $A = \frac{1}{a}A'$, whence the statement. □

Now I drop the assumption that ρ is irreducible. Let $\lambda_1, \ldots, \lambda_r$ be the distinct highest weights of ρ. For $1 \leq j \leq r$ let $v_{j,1}, \ldots, v_{j,m_j}$ be a linearly independent set of highest weight vectors of highest weight λ_j. So each $v_{j,l}$ generates an irreducible $\mathfrak{g}^c$-submodule, denoted $V(\lambda_j, l)$, of V^c, and V^c is their direct sum. We use the basis of V^c consisting of the elements $\rho(y_{i_1}) \cdots \rho(y_{i_k})v_{j,l}$, for $(i_1, \ldots, i_k) \in S_{\lambda_j}$. For $1 \leq j \leq r$ and $1 \leq s, t \leq m_j$ we let $A_j^{s,t}$ be the linear map $V^c \to V^c$ that maps $\rho(y_{i_1}) \cdots \rho(y_{i_k})v_{j,s}$ to $\rho(y_{i_1}) \cdots \rho(y_{i_k})v_{j,t}$ for $(i_1, \ldots, i_k) \in S_{\lambda_j}$, and it maps all other basis elements to 0. Then $A_j^{s,t}$ is an isomorphism of $V(\lambda_j, s)$ to $V(\lambda_j, t)$, and it maps all other submodules $V(\lambda_k, u)$ to 0. So by Lemma 5.2, $A_j^{s,t}\rho(x) = \rho(x)A_j^{s,t}$ for all $x \in \mathfrak{g}^c$, i.e., it is contained in

$$\mathrm{End}_\rho(V^c) = \{A \in \mathrm{End}(V^c) \mid A\rho(x) = \rho(x)A \text{ for all } x \in \overset{c}{\mathfrak{g}}\}.$$

Lemma 5.3. *The $A_j^{s,t}$ for $1 \leq j \leq r$ and $1 \leq s, t \leq m_j$ form a basis of* $\mathrm{End}_\rho(V^c)$.

Proof. Let $A \in \mathrm{End}_\rho(V^c)$. Then A is determined by the images $Av_{j,s}$ for $1 \leq j \leq r$, $1 \leq s \leq m_j$. But A maps (highest) weight vectors to (highest) weight vectors of the same weight. So there are $\alpha_j^{s,t} \in \mathbb{C}$ such that

$$Av_{j,s} = \alpha_j^{s,1}v_{j,1} + \cdots + \alpha_j^{s,m_j}v_{j,m_j}.$$

It follows that $A = \sum_{j,s,t} \alpha_j^{s,t}A_j^{s,t}$. It is obvious that the $A_j^{s,t}$ are linearly independent. □

Now consider a second representation $\varphi : \mathfrak{g}^c \to \mathfrak{gl}(V^c)$ that is equivalent to ρ, i.e., there is a bijective linear map $A_0 : V^c \to V^c$ such that $A_0\rho(x) = \varphi(x)A_0$ for all $x \in \mathfrak{g}^c$. In particular, A_0 lies in the space

$$\mathrm{End}_{\rho,\varphi}(V^c) = \{A \in \mathrm{End}(V^c) \mid A\rho(x) = \varphi(x)A \text{ for all } x \in \overset{c}{\mathfrak{g}}\}.$$

We want to find a basis of $\mathrm{End}_{\rho,\varphi}(V^c)$. A first observation is that $\mathrm{End}_{\rho,\varphi}(V^c) = \{A_0A \mid A \in \mathrm{End}_\rho(V^c)\}$. So since above we have seen how to construct a basis of $\mathrm{End}_\rho(V^c)$, the problem boils down to constructing A_0. Since φ is equivalent to ρ there are $w_{j,1}, \ldots, w_{j,m_j}$ forming a basis of the weight space with weight λ_j, relative to the representation φ. Applying Lemma 5.2 to each submodule $V(\lambda_j, l)$ we see that mapping $v_{j,l}$ to $w_{j,l}$ (for all j, l) uniquely extends to a bijective linear map $A_0 : V^c \to V^c$, contained in $\mathrm{End}_{\rho,\varphi}(V^c)$.

5.1.1 On solving polynomial equations

In the end, the solution to our problem will be given by a set of polynomial equations, which we need to solve. For this, to the best of our knowledge, no good algorithm is available. So in each particular case we have to look at the equations and see whether we can solve them. However, there are some algorithms that can help with that, most importantly the algorithm for constructing a Gröbner basis (see [52]). Let F be a field, and $R = F[x_1, \ldots, x_m]$ the polynomial ring in m indeterminates over F. Let $P \subset R$ be a finite set of polynomials, and consider the polynomial equations $p = 0$ for $p \in P$. We want to determine the set $V = \{v \in F^m \mid p(v) = 0 \text{ for all } p \in P\}$. Let G be any other generating set of the ideal I of R generated by P. Then solving $p = 0$ for all $p \in P$ is equivalent to solving $g = 0$ for all $g \in G$ (the set of solutions is the same). A convenient choice for G is a Gröbner basis of I with respect to a lexicographical monomial order. Then G has a triangular form, which, in most cases, makes solving the equations easier. We refer to [52] for a more detailed discussion.

5.2 Construction of embeddings

Here we turn to our main problem, stated at the beginning of the chapter.
Let $\mathfrak{g}^c$, $\tilde{\mathfrak{g}}^c$ be complex semisimple Lie algebras, and suppose that we have an embedding $\varepsilon : \mathfrak{g}^c \hookrightarrow \tilde{\mathfrak{g}}^c$. Let $\mathfrak{h}^c$ be a fixed Cartan subalgebra of $\mathfrak{g}^c$, and let Φ denote the corresponding root system. Let $h_1, \ldots, h_\ell$, and x_α for $\alpha \in \Phi$ be a Chevalley basis of $\mathfrak{g}^c$. Let $\mathfrak{u}$ be the compact form spanned by the elements (X_α, Y_α, H_α), with corresponding conjugation τ. Let $\mathfrak{g}$ be a real form of $\mathfrak{g}^c$ with Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$, and corresponding involution θ, and conjugation σ. We assume that $\mathfrak{g}$ and $\mathfrak{u}$ are compatible, i.e., τ and σ commute, and $\theta = \tau\sigma$ and $\mathfrak{u} = \mathfrak{k} \oplus \imath\mathfrak{p}$.

Proposition 5.4. *Let $\tilde{\mathfrak{g}} \subset \tilde{\mathfrak{g}}^c$ be a real form of $\tilde{\mathfrak{g}}^c$ such that $\varepsilon(\mathfrak{g}) \subset \tilde{\mathfrak{g}}$. Then there are a compact form $\tilde{\mathfrak{u}} \subset \tilde{\mathfrak{g}}^c$ of $\tilde{\mathfrak{g}}^c$, with conjugation $\tilde{\tau} : \tilde{\mathfrak{g}}^c \to \tilde{\mathfrak{g}}^c$, and an involution $\tilde{\theta}$ of $\tilde{\mathfrak{g}}^c$ such that*

1. *$\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$,*
2. *$\varepsilon\theta = \tilde{\theta}\varepsilon$,*
3. *$\tilde{\theta}\tilde{\tau} = \tilde{\tau}\tilde{\theta}$,*
4. *there is a Cartan decomposition $\tilde{\mathfrak{g}} = \tilde{\mathfrak{k}} \oplus \tilde{\mathfrak{p}}$, such that the restriction of $\tilde{\theta}$ to $\tilde{\mathfrak{g}}$ is the corresponding Cartan involution, and $\tilde{\mathfrak{u}} = \tilde{\mathfrak{k}} \oplus \imath\tilde{\mathfrak{p}}$.*

Conversely, if $\tilde{\mathfrak{u}} \subset \tilde{\mathfrak{g}}$ is a compact form, with corresponding conjugation $\tilde{\tau}$, and $\tilde{\theta}$ is an involution of $\tilde{\mathfrak{g}}^c$ such that (1), (2) *and* (3) *hold, then $\tilde{\theta}$ leaves $\tilde{\mathfrak{u}}$ invariant, and setting $\tilde{\mathfrak{k}} = \tilde{\mathfrak{u}}_1$, $\tilde{\mathfrak{p}} = \imath\tilde{\mathfrak{u}}_{-1}$ (where $\tilde{\mathfrak{u}}_k$ is the k-eigenspace of $\tilde{\theta}$), we get that $\tilde{\mathfrak{g}} = \tilde{\mathfrak{k}} \oplus \tilde{\mathfrak{p}}$ is a real form of $\tilde{\mathfrak{g}}^c$ with $\varepsilon(\mathfrak{g}) \subset \tilde{\mathfrak{g}}$.*

Proof. There is a Cartan decomposition $\tilde{\mathfrak{g}} = \tilde{\mathfrak{k}} \oplus \tilde{\mathfrak{p}}$ such that $\varepsilon(\mathfrak{k}) \subset \tilde{\mathfrak{k}}$, $\varepsilon(\mathfrak{p}) \subset \tilde{\mathfrak{p}}$ (this is the Karpelevich-Mostow theorem, see [63], §6, Corollary 1). We let $\tilde{\theta}$ be the involution of $\tilde{\mathfrak{g}}^c$ such that $\tilde{\theta}(x) = x$ for all $x \in \tilde{\mathfrak{k}}^c$, and $\tilde{\theta}(x) = -x$ for all $x \in \tilde{\mathfrak{p}}^c$. Finally we set $\tilde{\mathfrak{u}} = \tilde{\mathfrak{k}} \oplus \imath\tilde{\mathfrak{p}}$. Then the statements (1), (2), (3), and (4) are all obvious. The converse is clear as well. □

Throughout this section let $\tilde{\mathfrak{h}}^c$ be a fixed Cartan subalgebra of $\tilde{\mathfrak{g}}^c$. We let Ψ denote the root system of $\tilde{\mathfrak{g}}^c$ with respect to $\tilde{\mathfrak{h}}^c$. By $g_1, \ldots, g_m$ together with y_β, for $\beta \in \Psi$ we denote a fixed Chevalley basis of $\tilde{\mathfrak{g}}^c$. We let $\tilde{\mathfrak{u}}$ be the compact form of $\tilde{\mathfrak{g}}^c$ spanned by $\imath g_i$, $1 \leq i \leq m$, $y_\beta - y_{-\beta}$, $\imath(y_\beta + y_{-\beta})$ for $\beta \in \Psi^+$.
From the formulation of the main problem we see that it does not make a difference if we replace ε by $\phi\varepsilon$, where $\phi \in \mathrm{Aut}(\tilde{\mathfrak{g}}^c)$. The first step of our procedure is to replace ε by a $\phi\varepsilon$ to ensure that $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$. This is the subject of Section 5.3.
In Section 5.4 we show how to find the involutions $\tilde{\theta}$ with Proposition 5.4(2) and (3). Then Proposition 5.4 shows how to construct the corresponding real forms of $\tilde{\mathfrak{g}}^c$.
We recall [57], (see also [62], [70]) that:

Definition 25. Two embeddings $\varepsilon, \varepsilon' : \mathfrak{g}^c \hookrightarrow \tilde{\mathfrak{g}}^c$ are called **equivalent** if there is an *inner* automorphism ϕ of $\tilde{\mathfrak{g}}^c$ such that $\varepsilon = \phi\varepsilon'$.
They are called **linearly equivalent** if for all representations $\rho : \tilde{\mathfrak{g}}^c \to \mathfrak{gl}(V^c)$ the induced representations $\rho \circ \varepsilon$, $\rho \circ \varepsilon'$ are equivalent.

Equivalence implies linear equivalence, but the converse is not always true. However, the cases where the same linear equivalence class splits into more than one equivalence class are rather rare (cf. [62], Theorem 7).

5.3 Embedding the compact form

Suppose that $\varepsilon(\mathfrak{h}^c) \subset \tilde{\mathfrak{h}}^c$. Then for $\alpha \in \Phi$ there is a subset $A_\alpha \subset \Psi$ such that

$$\begin{aligned} \varepsilon(x_\alpha) &= \sum_{\beta \in A_\alpha} a_{\alpha,\beta} y_\beta \\ \varepsilon(x_{-\alpha}) &= \sum_{\beta \in A_\alpha} b_{\alpha,\beta} y_{-\beta}, \end{aligned} \tag{5.1}$$

where $a_{\alpha,\beta}, b_{\alpha,\beta} \in \mathbb{C}$ (in fact, A_α consists of all β which restricted to $\varepsilon(\mathfrak{h}^c)$ equal α).

Definition 26. We say that the embedding ε is **balanced** if $\varepsilon(\mathfrak{h}^c) \subset \tilde{\mathfrak{h}}^c$ and for all $\alpha \in \Phi$, and $\beta \in A_\alpha$ we have $b_{\alpha,\beta} = \bar{a}_{\alpha,\beta}$ (complex conjugation).

Of course, this notion depends on the choices of Cartan subalgebras and Chevalley bases in $\mathfrak{g}^c$, $\tilde{\mathfrak{g}}^c$. If we use the term "balanced" without mentioning these, then we use the choices fixed at the outset. Otherwise we explicitly mention a different choice made.

Lemma 5.5. *If ε is balanced then $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$. Conversely, if $\varepsilon(\mathfrak{h}^c) \subset \tilde{\mathfrak{h}}^c$ and $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$, then ε is balanced.*

Proof. By standard arguments one can show that $\varepsilon(h_i)$ is a $\mathbb{Q}$-linear combination of the g_j. (Set $x = \varepsilon(x_{\alpha_i})$, $y = \varepsilon(x_{-\alpha_i})$, $h = \varepsilon(h_i)$. Then $[x, y] = h$, $[h, x] = 2x$, $[h, y] = -2y$. So by $\mathfrak{sl}_2$-representation theory the eigenvalues of $\mathrm{ad}_{\tilde{\mathfrak{g}}^c} h$ are integers. Let $\{\beta_1, \ldots, \beta_m\}$ be a basis of simple roots of Ψ, with corresponding Cartan matrix $\widetilde{C}$. Then $\beta_j(h) \in \mathbb{Z}$ for all j. Furthermore, if we write $h = a_1 g_1 + \cdots + a_m g_m$, then we get that the vector $(a_1, \ldots, a_m)$ is $\widetilde{C}^{-1}$ times the vector $(\beta_1(h), \ldots, \beta_m(h))$. So $a_j \in \mathbb{Q}$.) In particular, $\varepsilon(\imath h_i)$ lies in the $\mathbb{R}$-span of $\imath g_1, \ldots, \imath g_m$.

Also, for $\alpha \in \Phi^+$ we have

$$\begin{aligned}\varepsilon(x_\alpha - x_{-\alpha}) &= \sum_{\beta \in A_\alpha} a_{\alpha,\beta} y_\beta - b_{\alpha,\beta} y_{-\beta} \\ &= \sum_{\beta \in A_\alpha} \frac{a_{\alpha,\beta} + b_{\alpha,\beta}}{2}(y_\beta - y_{-\beta}) - \imath \frac{a_{\alpha,\beta} - b_{\alpha,\beta}}{2} \imath (y_\beta + y_{-\beta}).\end{aligned} \tag{5.2}$$

We see that all coefficients lie in $\mathbb{R}$, whence $\varepsilon(x_\alpha - x_{-\alpha}) \in \tilde{\mathfrak{u}}$. The argument for $\varepsilon(\imath(x_\alpha + x_{-\alpha}))$ is entirely similar.
For the converse, from (5.2) we get that $a_{\alpha,\beta} + b_{\alpha,\beta} \in \mathbb{R}$ and $a_{\alpha,\beta} - b_{\alpha,\beta} \in \imath\mathbb{R}$. That implies $b_{\alpha,\beta} = \bar{a}_{\alpha,\beta}$. □

The next lemma says that the automorphism that we are after exists.

Lemma 5.6. *There exists an inner automorphism ϕ of $\tilde{\mathfrak{g}}^c$ such that $\phi\varepsilon$ is balanced.*

Proof. There is a compact form $\tilde{\mathfrak{u}}'$ of $\tilde{\mathfrak{g}}^c$ such that $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}'$ ([63], §6, Proposition 3). There is an inner automorphism ϕ' of $\tilde{\mathfrak{g}}^c$ such that $\phi'(\tilde{\mathfrak{u}}') = \tilde{\mathfrak{u}}$ ([63], §3, Corollary to Proposition 6). Moreover, the span of the elements $\phi'(\varepsilon(\imath h_i))$ lies in a Cartan subalgebra of $\tilde{\mathfrak{u}}$, which is conjugate to the span of the $\imath g_j$ by an inner automorphism of $\tilde{\mathfrak{u}}$. This automorphism extends to an inner automorphism of $\tilde{\mathfrak{g}}^c$. So we get an inner automorphism ϕ of $\tilde{\mathfrak{g}}^c$ such that $\phi(\varepsilon(\mathfrak{u})) \subset \tilde{\mathfrak{u}}$, and $\phi(\varepsilon(\mathfrak{h}^c)) \subset \tilde{\mathfrak{h}}^c$. So by Lemma 5.5 we conclude that $\phi\varepsilon$ is balanced. □

Now suppose that ε has the property that $\varepsilon(\mathfrak{h}^c) \subset \tilde{\mathfrak{h}}^c$, but ε is not balanced. Let $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ be a fixed basis of simple roots of Φ. Then we set up a system of polynomial equations. The indeterminates are $s_{\alpha,\beta}$, $t_{\alpha,\beta}$, where $\alpha \in \Delta$, $\beta \in A_\alpha$. For $1 \leq i \leq \ell$ we set

$$\begin{aligned}X_i &= \sum_{\beta \in A_{\alpha_i}} (s_{\alpha_i,\beta} + \imath t_{\alpha_i,\beta}) y_\beta \\ Y_i &= \sum_{\beta \in A_{\alpha_i}} (s_{\alpha_i,\beta} - \imath t_{\alpha_i,\beta}) y_{-\beta}\end{aligned}$$

Next we require that the 3ℓ elements $\varepsilon(h_i)$, X_i, Y_i satisfy the relations (3.1) (where in place of g_i we take $\varepsilon(h_i)$, in place of x_i, y_i we take X_i, Y_i). This leads to a set of polynomial equations in the indeterminates $s_{\alpha,\beta}$, $t_{\alpha,\beta}$, which we solve over $\mathbb{R}$. Let $\hat{s}_{\alpha,\beta}, \hat{t}_{\alpha,\beta} \in \mathbb{R}$ be the values that we obtain. Let $\widehat{X}_i$, $\widehat{Y}_i$ be the same as X_i, Y_i, but with these values substituted. Then mapping h_i to $\varepsilon(h_i)$, x_{α_i} to $\widehat{X}_i$, $x_{-\alpha_i}$ to $\widehat{Y}_i$ defines an embedding $\hat{\varepsilon} : \mathfrak{g}^c \to \tilde{\mathfrak{g}}^c$ (see Section 3.2.2).

Lemma 5.7. *$\hat{\varepsilon}$ is balanced.*

Proof. Consider the elements $x_\alpha - x_{-\alpha}$, $\imath(x_\alpha + x_{-\alpha})$, for $\alpha \in \Delta$ and $\imath h_i$, for $1 \leq i \leq \ell$. The span of these over $\mathbb{C}$ is the same as the span of the canonical generating set consisting of the x_α, $x_{-\alpha}$, h_i. So they generate $\mathfrak{g}^c$ over $\mathbb{C}$, and since they lie in $\mathfrak{u}$, they generate $\mathfrak{u}$ over $\mathbb{R}$. Moreover, their images under $\hat{\varepsilon}$ lie in $\tilde{\mathfrak{u}}$, so $\hat{\varepsilon}(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$. Since also $\hat{\varepsilon}(\mathfrak{h}^c) \subset \tilde{\mathfrak{h}}^c$ we conclude by Lemma 5.5. □

Since $\hat{\varepsilon}$ agrees with ε on $\mathfrak{h}^c$, we have that ε and $\hat{\varepsilon}$ are linearly equivalent (see [57], Theorem 1.5, see also [70], Theorem 4). If the linear equivalence class of ε does not split into more than one equivalence class, then we are done: ε and ε' are equivalent. If we are in a rare case where there are more equivalence classes, then we have to find more solutions to the polynomial equations: one for each equivalence class contained in the linear equivalence class of ε.

Remark 5.8. For the embeddings that have been determined with the methods of [70], the following trick often works. Let $\Pi = \{\beta_1, \ldots, \beta_m\}$ be a fixed basis of simple roots of Ψ. Let $\delta_1, \ldots, \delta_m \in \mathbb{C}\backslash\{0\}$, and let ϕ be the automorphism of $\tilde{\mathfrak{g}}^c$ mapping $g_j \mapsto g_j$, $y_{\beta_j} \mapsto \delta_j y_{\beta_j}$ $y_{-\beta_j} \mapsto \delta_j^{-1} y_{-\beta_j}$. Then the images of the g_j, and y_β under ϕ also form a Chevalley basis of $\tilde{\mathfrak{g}}^c$. Moreover, $\phi(y_\beta) = \delta_1^{e_1} \cdots \delta_m^{e_m} y_\beta$, if $\beta = \sum_j e_j \beta_j$. Write $y'_\beta = \phi(y_\beta) = \delta_\beta y_\beta$.
Now consider the equations (5.1), and write $b_{\alpha,\beta} = \mu_{\alpha,\beta} \bar{a}_{\alpha,\beta}$. If we use the basis consisting of the y'_β, then we get that the coefficients are $a'_{\alpha,\beta} = \delta_\beta^{-1} a_{\alpha,\beta}$ and $b'_{\alpha,\beta} = \delta_\beta b_{\alpha,\beta}$. So $b'_{\alpha,\beta} = \bar{a}'_{\alpha,\beta}$ is equivalent to $\delta_\beta^2 = \mu_{\alpha,\beta}^{-1}$. This then yields a set of polynomial equations for the δ_i. It is by no means guaranteed that this set is consistent (i.e., has any solution at all). However, from our experience, we get that in many cases the set is not only consistent, but also a reduced Gröbner basis is of the form $\{\delta_1^2 - r_1, \ldots, \delta_m^2 - r_m\}$, with $r_i \in \mathbb{R}$, $r_i > 0$, which makes solving the equations extremely easy.
A solution of the equations yields an automorphism ϕ of $\tilde{\mathfrak{g}}^c$ such that $\phi(\tilde{\mathfrak{u}}) = \tilde{\mathfrak{u}}'$, where $\tilde{\mathfrak{u}}'$ is the compact form spanned by the elements $\imath g_j$, $y'_\beta - y'_{-\beta}$, $\imath(y'_\beta + y'_{-\beta})$. Moreover, ε is balanced with respect to the Chevalley basis consisting of the y'_β, so that $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}'$. So if we set $\varepsilon' = \phi^{-1}\varepsilon$, then ε' is equivalent to ε and $\varepsilon'(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$.

5.4 Finding $\tilde{\theta}$

Here we assume that we have an embedding $\varepsilon : \mathfrak{g}^c \hookrightarrow \tilde{\mathfrak{g}}^c$ such that $\varepsilon(\mathfrak{h}^c) \subset \tilde{\mathfrak{h}}^c$ and $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$. Now we focus on the problem of finding the involutions $\tilde{\theta}$ of $\tilde{\mathfrak{g}}^c$ such that $\varepsilon\theta = \tilde{\theta}\varepsilon$.
Let $\operatorname{ad} : \tilde{\mathfrak{g}}^c \to \mathfrak{gl}(\tilde{\mathfrak{g}}^c)$ be the adjoint representation, i.e., $\operatorname{ad} x(y) = [x, y]$. Set

$$\mathcal{A} = \{A \in \operatorname{End}(\tilde{\mathfrak{g}}^c) \mid A \operatorname{ad}(\varepsilon\theta(y)) = \operatorname{ad}(\varepsilon(y))A \text{ for all } y \in \overset{c}{\mathfrak{g}}\}.$$

Proposition 5.9. *Let $\tilde{\theta} \in \operatorname{End}(\tilde{\mathfrak{g}}^c)$. Then $\tilde{\theta}$ is an involution of $\tilde{\mathfrak{g}}^c$ with $\varepsilon\theta = \tilde{\theta}\varepsilon$ if and only if $\tilde{\theta} \in \mathcal{A}$ and*

1. *$\tilde{\theta}^2 = I$, where $I \in \operatorname{End}(\tilde{\mathfrak{g}}^c)$ is the identity,*
2. *$\tilde{\theta}(\operatorname{ad} x)\tilde{\theta} = \operatorname{ad}\tilde{\theta}(x)$ for all $x \in \tilde{\mathfrak{g}}^c$.*

Proof. Suppose that $\tilde{\theta}$ is an involution of $\tilde{\mathfrak{g}}^c$. Then (1) is immediate. Also for $y \in \tilde{\mathfrak{g}}^c$ we have $\tilde{\theta}(\operatorname{ad} x)\tilde{\theta}(y) = \tilde{\theta}[x, \tilde{\theta}(y)] = \operatorname{ad}\tilde{\theta}(x)(y)$, so (2) follows. Together with $\varepsilon\theta = \tilde{\theta}\varepsilon$ this also implies that $\tilde{\theta} \in \mathcal{A}$.
For the converse we first show that $\tilde{\theta}$ is an involution of $\tilde{\mathfrak{g}}^c$. From (1) it follows that it is bijective and that it has order 2. Using (2) we get $\tilde{\theta}[x, y] = \tilde{\theta} \operatorname{ad} x(y) = \operatorname{ad}\tilde{\theta}x(\tilde{\theta}y) = [\tilde{\theta}(x), \tilde{\theta}(y)]$. Secondly, $\tilde{\theta}\varepsilon = \varepsilon\theta$ is equivalent to $\operatorname{ad}\tilde{\theta}\varepsilon(y) = \operatorname{ad}\varepsilon\theta(y)$ for all $y \in \mathfrak{g}^c$. Using (1) and (2) it is straightforward to see that this is the same as $\tilde{\theta} \in \mathcal{A}$. □

We let $a_1, \ldots, a_n$ be a fixed basis of $\tilde{\mathfrak{g}}^c$ (for example, the Chevalley basis fixed at the start). The idea now is to translate the conditions of Proposition 5.9 into polynomial equations. For that we proceed as follows:

1. Compute a basis $A_1, \ldots, A_s$ of $\mathcal{A}$ (see Section 5.1; note that, if we let $\rho, \varphi : \mathfrak{g}^c \to \mathfrak{gl}(\tilde{\mathfrak{g}}^c)$ be the representations given by $\rho(y) = \operatorname{ad} \varepsilon\theta(y)$, $\varphi(y) = \operatorname{ad} \varepsilon(y)$, then $\mathcal{A} = \operatorname{End}_{\rho,\varphi}(\tilde{\mathfrak{g}}^c)$).

2. Let $z_1, \ldots, z_s$ be indeterminates over $\mathbb{C}$, and set $A = z_1A_1 + \cdots + z_sA_s$. Then $A^2 = I$ is equivalent to a set of polynomial equations in the z_i. Let P_1 denote the corresponding set of polynomials.

3. We note that Proposition 5.9(2) is equivalent to $A \operatorname{ad} a_j A = \operatorname{ad} Aa_j$ for $1 \leq j \leq n$. Also this is equivalent to a set of polynomial equations in the z_i. Let P_2 denote the corresponding set of polynomials.

Now we consider the compact form $\tilde{\mathfrak{u}}$, and the corresponding conjugation $\tilde{\tau} : \tilde{\mathfrak{g}}^c \to \tilde{\mathfrak{g}}^c$. We want to construct involutions $\tilde{\theta}$ of $\tilde{\mathfrak{g}}^c$ that commute with $\tilde{\tau}$ (or, equivalently, that leave $\tilde{\mathfrak{u}}$ invariant). First we observe that it is straightforward to compute $\tilde{\tau}(x)$ for an $x \in \tilde{\mathfrak{g}}^c$. Indeed, let $u_1, \ldots, u_n$ be a basis of $\tilde{\mathfrak{u}}$, and write $x = \sum_i \alpha_i u_i$, with $u_i \in \mathbb{C}$. Then $\tilde{\tau}(x) = \sum_i \bar{\alpha}_i u_i$.
Let $R = \mathbb{R}[x_1, \ldots, x_s, y_1, \ldots, y_s]$. We substitute $x_i + \imath y_i$ for z_i in the polynomials in the sets P_1, P_2. A polynomial f in one of these sets then transforms into $g + \imath h$, with $g, h \in R$. The polynomial equation $f = 0$ is equivalent to two polynomial equations, this time over $\mathbb{R}$, $g = h = 0$. This way we obtain a set of polynomials $Q_1 \subset R$.
Let $A = \sum_{i=1}^{s}(x_i + \imath y_i)A_i$, then $\tilde{\tau}A(a_j) = A\tilde{\tau}(a_j)$ is the same as

$$\sum_{i=1}^{n}(x_i - \imath y_i)\tilde{\tau}(A_i a_j) = \sum_{i=1}^{n}(x_i + \imath y_i)A_i\tilde{\tau}(a_j).$$

Again we split the real and imaginary parts. Doing this for $1 \leq j \leq n$ we obtain a system of (linear) polynomial equations. The corresponding set of polynomials is denoted by Q_2.
Finally we solve the system of polynomial equations $q = 0$ for $q \in Q_1 \cup Q_2$. Let $\tilde{\mathfrak{g}}_1, \ldots, \tilde{\mathfrak{g}}_m$ be fixed noncompact real forms of $\tilde{\mathfrak{g}}^c$, such that each noncompact real form of $\tilde{\mathfrak{g}}^c$ is isomorphic to exactly one of the $\tilde{\mathfrak{g}}_i$. Each solution of the polynomial equations yields an involution $\tilde{\theta}$ of $\tilde{\mathfrak{g}}^c$, and we construct the corresponding real form $\tilde{\mathfrak{g}}$ as in Proposition 5.4. The using the methods of [54] we find an isomorphism $\tilde{\mathfrak{g}} \to \tilde{\mathfrak{g}}_i$, and hence we can map $\mathfrak{g}$ to a subalgebra of an appropriate $\tilde{\mathfrak{g}}_i$.

Remark 5.10. This method works best when the polynomial equations have a finite set of solutions: we list them all, and obtain all $\tilde{\mathfrak{g}}_i$ such that $\mathfrak{g}$ maps to a subalgebra by an automorphism of $\tilde{\mathfrak{g}}^c$. However, it can happen that the set of solutions is infinite. Example 5.11 describes a situation where we can deal with that.

5.5 Implementation and examples

As stated in the introduction, we have implemented the algorithms described here in the computer algebra system GAP4, using the package CoReLG. The main bottleneck of the method is the need to solve a system of polynomial equations. One of the main parameters influencing the complexity of this system is the dimension of the space $\mathcal{A}$, since the number of indeterminates is $2\dim\mathcal{A}$. (Although, of course, there are also some linear equations, effectively reducing the number of indeterminates.) From Section 5.1 we see that $\dim\mathcal{A} = \sum_{i=1}^{r} m_i^2$, where the m_i are the multiplicities of the irreducible $\mathfrak{g}^c$-submodules of $\tilde{\mathfrak{g}}^c$. It can happen that $\dim\mathcal{A}$ is so large that the polynomial equations become unwieldy. For example, if $\varepsilon(\mathfrak{g}^c)$ is the regular subalgebra of type A_1+A_1 of F_4, then $\dim\mathcal{A} = 159$. On the other hand, there are many subalgebras that lead to equations systems that we can deal with. In this section we give some examples. An especially favorable situation arises when $\varepsilon(\mathfrak{g}^c)$ is an S-subalgebra. That will be the subject of the next section.
In the last two examples we also report on the Runtimes. They have been obtained on a 3.16 GHz processor. We remark here that there are two fundamental inefficiencies affecting these Runtimes: firstly, we work over a field containing the square root of all integers. This field has been implemented by ourselves in GAP (see [55]); however, since there is no GAP kernel support for it, computations using this field tend to take markedly longer that, say, over $\mathbb{Q}$. Secondly, we create a lot of polynomials, and also the polynomial arithmetic in GAP is not the most efficient possible (essentially for the same reason as for our field).

Example 5.11. Let $\tilde{\mathfrak{g}}^c$, $\mathfrak{g}^c$ be the Lie algebras of type A_3 and A_2 respectively. We consider the simplest possible embedding: Let $\alpha_1, \alpha_2, \alpha_3$ denote the simple roots of the root system of $\tilde{\mathfrak{g}}^c$, ordered as usual; then the subalgebra generated by $x_{\alpha_i}, x_{-\alpha_i}$ for $i = 1, 2$ is isomorphic to $\mathfrak{g}^c$. We consider the real form of $\mathfrak{g}^c$ isomorphic to $\mathfrak{sl}_3(\mathbb{R})$ (i.e., the split form).
Since the image of $\mathfrak{g}^c$ in $\tilde{\mathfrak{g}}^c$ is regular, i.e., is generated by root vectors of $\tilde{\mathfrak{g}}^c$, it is automatic that $\varepsilon(\mathfrak{u}) \subset \tilde{\mathfrak{u}}$.
In this case $\mathcal{A}$ has dimension 4. We get a set of 46 polynomial equations in the unknowns x_i, y_i, $1 \le i \le 4$. The reduced Gröbner basis of the ideal generated by these polynomials is

$$\{x_1 - 1, x_2 - x_3, x_3^2 + y_3^2 - 1, x_4 + 1, y_1, y_2 + y_3, y_4\}.$$

So there is an infinite number of solutions. Now we set $z_1 = 1$, $z_2 = x_3 - \imath y_3$, $z_3 = x_3 + \imath y_3$, $z_4 = -1$ (i.e., we work symbolically with x_3, y_3) and $A = z_1A_1 + \cdots + z_4A_4$. Then the characteristic polynomial of A is

$$T^{15}+3T^{14}+(-3x_3^2-3y_3^2)T^{13}+\cdots+(3x_3^6+9x_3^4y_3^2+9x_3^2y_3^4+3y_3^6)T+x_3^6+3x_3^4y_3^2+3x_3^2y_3^4+y_3^6.$$

However, using $x_3^2 + y_3^2 = 1$, this reduces to

$$T^{15} + 3T^{14} - 3T^{13} - 17T^{12} - 3T^{11} + 39T^{10} + 25T^9 - 45T^8 - 45T^7 + 25T^6 + 39T^5 - 3T^4 - 17T^3 - 3T^2 + 3T + 1$$

which is $(T-1)^6(T+1)^9$. From this we conclude that if we take any solution of the equations and construct the corresponding real form $\tilde{\mathfrak{g}}$, then its Cartan decomposition will be $\tilde{\mathfrak{g}} = \tilde{\mathfrak{k}} \oplus \tilde{\mathfrak{p}}$ with $\dim\tilde{\mathfrak{k}} = 6$ and $\dim\tilde{\mathfrak{p}} = 9$.

Now there is, up to isomorphism, only one real form of $\tilde{\mathfrak{g}}^c$ with a Cartan decomposition satisfying this, namely $\mathfrak{sl}_4(\mathbb{R})$. Also, up to equivalence, $\tilde{\mathfrak{g}}^c$ contains exactly one subalgebra isomorphic to $\mathfrak{g}^c$. So we conclude that $\mathfrak{sl}_4(\mathbb{R})$ is the only real form of $\tilde{\mathfrak{g}}^c$ containing a subalgebra isomorphic to $\mathfrak{sl}_3(\mathbb{R})$.

Example 5.12. Let $\tilde{\mathfrak{g}}^c$, $\mathfrak{g}^c$ be the Lie algebras of type E_8 and $A_1+G_2+G_2$ respectively. As real form $\mathfrak{g}$ we took the direct sum of the noncompact real forms of A_1 and G_2 (twice) respectively. In this case $\mathcal{A}$ was computed in 2058 seconds, and $\dim \mathcal{A} = 6$. The polynomial equations were computed in 36783 seconds. The set $Q_1 \cup Q_2$ contains 37460 polynomials. However, a reduced Gröbner basis of the ideal generated by them is

$$\{x_1+1, x_2, x_3-1, x_4+1, x_5-1, x_6+1, y_1, y_2, y_3, y_4, y_5, y_6\}.$$

So there is only one solution. The corresponding real form of E_8 turned out to be EVIII.

Example 5.13. Let $\tilde{\mathfrak{g}}^c$ be of type E_6. Then, up to equivalence, $\tilde{\mathfrak{g}}^c$ contains a unique subalgebra of type B_4. So let $\mathfrak{g}^c$ be of type B_4 and let $\mathfrak{g} = \mathfrak{so}(4,5)$. In this example $\mathcal{A}$ was computed in 55 seconds, and $\dim \mathcal{A} = 7$. The polynomial equations were computed in 510 seconds, the reduced Gröbner basis of the ideal generated by them is

$$\{x_5^2-x_7, x_5x_6, x_6^2+y_6^2+x_7-1, x_5x_7-x_5, x_6x_7, x_7^2-x_7, x_5y_6, x_7y_6, x_1+x_5, x_2+x_6, \\ x_3+1, x_4+x_7, y_1, y_2-y_6, y_3, y_4, y_5, y_7\}.$$

We see that x_7 can have the values 0,1. Adding x_7 to the generating set, the Gröbner basis becomes

$$\{x_6^2+y_6^2-1, x_1, x_2+x_6, x_3+1, x_4, x_5, x_7, y_1, y_2-y_6, y_3, y_4, y_5, y_7\}.$$

Here the value of x_6, y_6 determines the solution completely. Furthermore, there is an infinite number of possible values for those indeterminates. However, with the same method as in Example 5.11, we established that all solutions lead to the inclusion $\mathfrak{so}(4,5) \subset E$I.
Adding $x_7 - 1$ to the generating set, we get the Gröbner basis

$$\{x_5^2-1, x_1+x_5, x_2, x_3+1, x_4+1, x_6, x_7-1, y_1, y_2, y_3, y_4, y_5, y_6, y_7\}.$$

Here we get two solutions, which both yield the inclusion $\mathfrak{so}(4,5) \subset E$II.

5.6 S-subalgebras of the exceptional Lie algebras

In this section we consider embeddings $\varepsilon : \mathfrak{g}^c \hookrightarrow \tilde{\mathfrak{g}}^c$, such that $\varepsilon(\mathfrak{g}^c)$ is a maximal S-subalgebra of $\tilde{\mathfrak{g}}^c$, and the latter is of exceptional type.
Let $\mathfrak{g}$ be a real form of $\mathfrak{g}^c$. By [63], §6, Theorem 2, if $\varepsilon(\mathfrak{g}^c)$ is an S-subalgebra of $\tilde{\mathfrak{g}}^c$, then there are at most two real forms of $\tilde{\mathfrak{g}}^c$ that contain $\varepsilon(\mathfrak{g})$. And if $\tilde{\mathfrak{g}}^c$ has no outer automorphisms there is at most one such real form. This explains why our method works particularly well in this case: the polynomial equations have at most two solutions. Example 5.12 illustrates this phenomenon (there the subalgebra is a non maximal S-subalgebra).
Table 10 contains the results that we obtained using our programs (for the situation described above, i.e., $\varepsilon(\mathfrak{g}^c)$ is a maximal S-subalgebra of $\tilde{\mathfrak{g}}^c$). We describe the subalgebras of the complex simple Lie algebras by giving the type of their root systems, with an upper index denoting the Dynkin index (see [57]).

Komrakov [61] has also published a list of the S-subalgebras of the real simple Lie algebras of exceptional type. In type E_6 we find a few differences: the inclusions marked by a $(*)$ are not contained in Komrakov's list. About all other inclusions Komrakov's list and ours agree.

Table 10: Maximal S-subalgebras of the real Lie algebras of exceptional type.

complex inclusion	real inclusion
$A_2^9 \subset E_6$	$\begin{cases} \mathfrak{su}(1,2) \subset E\mathrm{II} \\ \mathfrak{sl}(3,\mathbb{R}) \subset E\mathrm{II} \end{cases}$
$G_2^3 \subset E_6$	$G \subset E\mathrm{II}$ (*)
$A_2^2 \oplus G_2^1 \subset E_6$	$\begin{cases} \mathfrak{su}(3) \oplus G^{cmp} \subset E\mathrm{I} \\ \mathfrak{su}(1,2) \oplus G \subset E\mathrm{III} \\ \mathfrak{su}(1,2) \oplus G^{cmp} \subset E\mathrm{II}(*) \\ \mathfrak{sl}(3,\mathbb{R}) \oplus G \subset E\mathrm{IV} \\ \mathfrak{sl}(3,\mathbb{R}) \oplus G^{cmp} \subset E\mathrm{I}(*) \end{cases}$
$C_4^1 \subset E_6$	$\begin{cases} \mathfrak{sp}(2,2) \subset E\mathrm{II}(*) \\ \mathfrak{sp}(2,2) \subset E\mathrm{IV}(*) \\ \mathfrak{sp}(1,3) \subset E\mathrm{III}(*) \\ \mathfrak{sp}(1,3) \subset E\mathrm{I}(*) \\ \mathfrak{sp}(4,\mathbb{R}) \subset E\mathrm{II}(*) \\ \mathfrak{sp}(4,\mathbb{R}) \subset E\mathrm{I}(*) \end{cases}$
$F_4^1 \subset E_6$	$\begin{cases} F\mathrm{I} \subset E\mathrm{I}(*) \\ F\mathrm{II} \subset E\mathrm{III}(*) \end{cases}$
$A_1^{231} \subset E_7$	$\mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{V}$
$A_1^{399} \subset E_7$	$\mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{V}$
$A_2^{21} \subset E_7$	$\begin{cases} \mathfrak{su}(1,2) \subset E\mathrm{VI} \\ \mathfrak{sl}(3,\mathbb{R}) \subset E\mathrm{V} \end{cases}$
$A_1^{15} \oplus A_1^{24} \subset E_7$	$\begin{cases} \mathfrak{su}(2) \oplus \mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{V} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus \mathfrak{su}(2) \subset E\mathrm{VI} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus \mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{VI} \end{cases}$
$A_1^7 \oplus G_2^2 \subset E_7$	$\begin{cases} \mathfrak{su}(2) \oplus G \subset E\mathrm{VI} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus G^{cmp} \subset E\mathrm{V} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus G \subset E\mathrm{V} \end{cases}$
$C_3^1 \oplus G_2^1 \subset E_7$	$\begin{cases} \mathfrak{sp}(3) \oplus G \subset E\mathrm{VI} \\ \mathfrak{sp}(1,2) \oplus G^{cmp} \subset E\mathrm{VI} \\ \mathfrak{sp}(1,2) \oplus G \subset E\mathrm{VI} \\ \mathfrak{sp}(3,\mathbb{R}) \oplus G^{cmp} \subset E\mathrm{VII} \\ \mathfrak{sp}(3,\mathbb{R}) \oplus G \subset E\mathrm{V} \end{cases}$

S-subalgebras	
$A_1^3 \oplus F_4^1 \subset E_7$	$\begin{cases} \mathfrak{su}(2) \oplus F\mathrm{I} \subset E\mathrm{VI} \\ \mathfrak{su}(2) \oplus F\mathrm{II} \subset E\mathrm{VI} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus F_4^{cmp} \subset E\mathrm{VII} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus F\mathrm{I} \subset E\mathrm{V} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus F\mathrm{II} \subset E\mathrm{VII} \end{cases}$
$A_1^{520} \subset E_8$	$\mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{VIII}$
$A_1^{760} \subset E_8$	$\mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{VIII}$
$A_1^{1240} \subset E_8$	$\mathfrak{sl}(2,\mathbb{R}) \subset E\mathrm{VIII}$
$B_2^{120} \subset E_8$	$\begin{cases} \mathfrak{so}(2,3) \subset E\mathrm{VIII} \\ \mathfrak{so}(4,1) \subset E\mathrm{VIII} \end{cases}$
$A_1^{16} \oplus A_2^6 \subset E_8$	$\begin{cases} \mathfrak{su}(2) \oplus \mathfrak{su}(1,2) \subset E\mathrm{VIII} \\ \mathfrak{su}(2) \oplus \mathfrak{sl}(3,\mathbb{R}) \subset E\mathrm{IX} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus \mathfrak{su}(3) \subset E\mathrm{VIII} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus \mathfrak{su}(1,2) \subset E\mathrm{VIII} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus \mathfrak{sl}(3,\mathbb{R}) \subset E\mathrm{VIII} \end{cases}$
$F_4^1 \oplus G_2^1 \subset E_8$	$\begin{cases} F_4^{cmp} \oplus G \subset E\mathrm{IX} \\ F\mathrm{I} \oplus G^{cmp} \subset E\mathrm{IX} \\ F\mathrm{I} \oplus G \subset E\mathrm{VIII} \\ F\mathrm{II} \oplus G^{cmp} \subset E\mathrm{VIII} \\ F\mathrm{II} \oplus G \subset E\mathrm{IX} \end{cases}$
$A_1^{156} \subset F_4$	$\mathfrak{sl}(2,\mathbb{R}) \subset F\mathrm{I}$
$A_1^8 \oplus G_2^1 \subset F_4$	$\begin{cases} \mathfrak{su}(2) \oplus G \subset F\mathrm{I} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus G^{cmp} \subset F\mathrm{II} \\ \mathfrak{sl}(2,\mathbb{R}) \oplus G \subset F\mathrm{I} \end{cases}$
$A_1^{28} \subset G_2$	$\mathfrak{sl}(2,\mathbb{R}) \subset G$

5.7 Regular semisimple subalgebras

As I said before the semisimple subalgebras of a semisimple Lie algebra have been the subject of many investigations. The main problem is to classify the semisimple subalgebras up to the action by the inner automorphism group.
For semisimple Lie algebras over the complex numbers this problem has only been fully solved for certain classes of subalgebras, such as regular subalgebras [57], maximal S-subalgebras ([57], [56]), simple subalgebras of the Lie algebras of exceptional type [62] and subalgebras isomorphic to $\mathfrak{sl}(2,\mathbb{C})$, using the theory of nilpotent orbits.
For semisimple Lie algebras over the real numbers the problem has been less investigated. Also for these algebras it is possible to obtain a list of subalgebras isomorphic to $\mathfrak{sl}(2,\mathbb{R})$, up to conjugacy by the inner automorphism group, by listing the nilpotent orbits (for this usually the Kostant-Sekiguchi correspondence is used, see [66], [55]). Furthermore, there are some publications ([50], [51], [67], [68]) where the following problem is considered: let $\mathfrak{a}^c$ be a semisimple subalgebra of the complex semisimple Lie algebra $\mathfrak{g}^c$, and let $\mathfrak{g}$ be a real form of $\mathfrak{g}^c$; and the question is which real forms of $\mathfrak{a}^c$ are contained in $\mathfrak{g}$. However, these articles contain no classifications up to the action of the inner automorphism group.

Definition 27. We recall that a subalgebra of a semisimple Lie algebra $\mathfrak{g}$ is said to be **regular** if it is normalized by a Cartan subalgebra of $\mathfrak{g}$.

In the next sections I give an algorithm to list the regular semisimple subalgebras of a semisimple real Lie algebra, up to conjugacy by the inner automorphism group. We have implemented this algorithm in the language of the computer algebra system GAP4. Using this implementation we have obtained the regular semisimple subalgebras of several real simple Lie algebras.

5.8 Cartan subalgebras

Let $\mathfrak{g}$ be a real semisimple Lie algebra, with adjoint group G. Let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ be a fixed Cartan decomposition of $\mathfrak{g}$.

Proposition 19. Every Cartan subalgebra of $\mathfrak{g}$ is G-conjugate to a θ-stable Cartan subalgebra. Moreover, up to G-conjugacy, there are a finite number of Cartan subalgebras in $\mathfrak{g}$.

In this section it is described how the methods of Sugiura yield an algorithm for finding a finite number of θ-stable Cartan subalgebras of $\mathfrak{g}$, such that every Cartan subalgebra of $\mathfrak{g}$ is G-conjugate to exactly one of them. This algorithm has been implemented in the CoReLG package.

Definition 28. Let $\mathfrak{h}$ be a θ-stable Cartan subalgebra of $\mathfrak{g}$. Then $\mathfrak{h} = \mathfrak{h} \cap \mathfrak{k} \oplus \mathfrak{h} \cap \mathfrak{p}$, and $\mathfrak{h} \cap \mathfrak{p}$ is called the **noncompact dimension** of $\mathfrak{h}$. Moreover,

$$\mathfrak{h} \cap \mathfrak{k} = \{h \in \mathfrak{h} \mid \mathrm{ad}_{\mathfrak{g}}\, h \text{ has only purely imaginary eigenvalues}\}$$
$$\mathfrak{h} \cap \mathfrak{p} = \{h \in \mathfrak{h} \mid \mathrm{ad}_{\mathfrak{g}}\, h \text{ has only real eigenvalues}\}$$

So we see that the noncompact dimension of $\mathfrak{h}$ can be defined without reference to the given Cartan decomposition. Hence it is a well-defined concept for non θ-stable Cartan subalgebras too.

Let $g \in G$ and $h \in \mathfrak{h}$, then $\mathrm{ad}_{\mathfrak{g}} h$ and $\mathrm{ad}_{\mathfrak{g}} g(h)$ have the same eigenvalues. We conclude that the noncompact dimension of $g(\mathfrak{h})$ equals that of $\mathfrak{h}$. Furthermore, all Cartan subalgebras of maximal noncompact dimension are G-conjugate.
Let $\mathfrak{h}$ be a θ-stable Cartan subalgebra of $\mathfrak{g}$. Let Φ denote the root system of $\mathfrak{g}^c$ with respect to $\mathfrak{h}^c$. We view Φ as a subset of the dual space $(\mathfrak{h}^c)^*$. Let W be the Weyl group of Φ. Set

$$N_{G^c}(\mathfrak{h}^c) = \{g \in G^c \mid g(h) \in \mathfrak{h}^c \text{ for all } h \in \mathfrak{h}^c\},$$
$$Z_{G^c}(\mathfrak{h}^c) = \{g \in G^c \mid g(h) = h \text{ for all } h \in \mathfrak{h}^c\}.$$

Let $\alpha \in \Phi$, e $g \in N_{G^c}(\mathfrak{h}^c)$. Set $\alpha^{g^{-1}} = \alpha \circ g^{-1}$. A straightforward argument shows that $g(\mathfrak{g}^c_\alpha) = \mathfrak{g}^c_{\alpha^{g^{-1}}}$. In particular, $\alpha^{g^{-1}} \in \Phi$.
So we get a map $\psi_g : \Phi \to \Phi$, $\psi_g(\alpha) = \alpha^{g^{-1}}$.

Theorem 5.14. *We have $\psi_g \in W$. The map $N_{G^c}(\mathfrak{h}^c) \to W$, $g \mapsto \psi_g$ is a surjective homomorphism of groups, with kernel $Z_{G^c}(\mathfrak{h}^c)$. In particular, $W \cong N_{G^c}(\mathfrak{h}^c)/Z_{G^c}(\mathfrak{h}^c)$.*

5.8.1 Computing the real Weyl group

Here $\mathfrak{g}$ is as in the previous subsection and $\mathfrak{h}$ is a θ-stable Cartan subalgebra of $\mathfrak{g}$.
We define $N_G(\mathfrak{h})$, $Z_G(\mathfrak{h})$ in a similar way to $N_{G^c}(\mathfrak{h}^c)$ and $Z_{G^c}(\mathfrak{h}^c)$.

Definition 29. Set $W(\mathfrak{h}) = N_G(\mathfrak{h})/Z_G(\mathfrak{h})$; this is called the **real Weyl group** of $\mathfrak{g}$ relative to $\mathfrak{h}$. We have that $W(\mathfrak{h})$ is a subgroup of W

An algorithm for finding generators of $W(\mathfrak{h})$ can be based on [65], Proposition 12.14. This algorithm has been implemented in the ATLAS software [64]. However, due to the various choices involved in describing a subgroup of W (the choice of a set of simple reflections, for example), it is not straightforward to translate the ATLAS output to our setting. Therefore, we describe a simple "brute-force" method for computing generators of $W(\mathfrak{h})$, that we used for the cases we considered.
Firstly, we have that $W(\mathfrak{h}) \subset W^\theta$, where the latter is the subgroup of elements commuting with θ. So the problem boils down to deciding whether, for a given $w \in W^\theta$, there exists a $g \in N_G(\mathfrak{h})$ projecting to w. For this we first define an element in $N_{G^c}(\mathfrak{h}^c)$ projecting to w.

Let Φ be the root system of $\mathfrak{g}^c$ with respect to $\mathfrak{h}^c$. Let $\{\alpha_1, \ldots, \alpha_\ell\}$ be a fixed set of simple roots. And let x_i, y_i, h_i, $1 \le i \le \ell$ form a corresponding canonical generating set. For $\alpha \in \Phi$ let $x_\alpha \in \mathfrak{g}^c_\alpha$ be the element of a Chevalley basis of $\mathfrak{g}^c$ such that $x_{\alpha_i} = x_i$, $x_{-\alpha_i} = y_i$. Then $x_{w(\alpha_i)}$, $x_{-w(\alpha_i)}$, $h_{w(\alpha_i)}$, $1 \le i \le \ell$, also form a canonical generating set. So mapping $x_i \mapsto x_{w(\alpha_i)}$, $y_i \mapsto x_{-w(\alpha_i)}$, $h_i \mapsto h_{w(\alpha_i)}$, defines an inner automorphism $\eta_w \in G^c$, whose restriction to $\mathfrak{h}$ equals w.
Now let $g \in Z_{G^c}(\mathfrak{h})$. Then $g(x_\alpha)$ is a multiple of x_α. So g is completely determined by ℓ nonzero parameters $\lambda_1, \ldots, \lambda_\ell$ such that $g(x_i) = \lambda_i x_i$, $g(y_i) = \lambda_i^{-1} y_i$. We denote this element by $\zeta_0(\lambda_1, \ldots, \lambda_\ell)$.
The set of all $g \in N_{G^c}(\mathfrak{h})$ whose restriction to $\mathfrak{h}$ equals w, is equal to the set of all $\eta_w \zeta_0(\lambda_1, \ldots, \lambda_l)$, where the $\lambda_i \in \mathbb{C}^*$. Furthermore, $w \in W(\mathfrak{h})$ if and only if there are nonzero λ_i such that $\eta_w \zeta_0(\lambda_1, \ldots, \lambda_l)$ lies in G, i.e., the entries of its matrix with respect to a basis of $\mathfrak{g}$ are real. Writing μ_i instead of λ_i^{-1}, the entries of this matrix are polynomials in the λ_i and μ_i (with coefficients in $\mathbb{C}$). Let $p \in \mathbb{C}[\lambda_1, \ldots, \lambda_\ell, \mu_1, \ldots, \mu_\ell]$ be such an entry. For λ_j we substitute $a_j + \imath b_j$, and for μ_j we substitute $c_j + \imath d_j$. Then we write $p = p_1 + \imath p_2$, where the p_k are polynomials in a_j, b_j, c_j, d_j, $1 \le j \le \ell$ with

coefficients in $\mathbb{R}$. We let P be the set of all p_2 that we obtain in this way, along with the polynomials $a_j c_j - b_j d_j - 1$, $a_j d_j + b_j c_j$ for $1 \leq j \leq \ell$. The conclusion is that $w \in W(\mathfrak{h})$ if and only if the set of polynomial equations $\{f = 0 \mid f \in P\}$ has a solution over $\mathbb{R}$.
Our method consists of writing down the set P, and explicitly finding a solution of the polynomial equations, or proving that none exist.

5.9 Dynkin's algorithm

Here we summarize Dynkin's algorithm [57] to list the semisimple subalgebras of a complex semisimple Lie algebra $\mathfrak{g}^c$, up to conjugacy by the adjoint group G^c.
Let $\mathfrak{h}^c$ be a fixed Cartan subalgebra of $\mathfrak{g}^c$. Since all Cartan subalgebras of $\mathfrak{g}^c$ are G^c-conjugate, it suffices to classify the $\mathfrak{h}^c$-regular subalgebras of $\mathfrak{g}^c$.
Let Φ be the root system of $\mathfrak{g}^c$ with respect to $\mathfrak{h}^c$. A set $\Gamma \subset \Phi$ is said to be a π-system if it is linearly independent, and $\alpha - \beta \notin \Phi$ for all $\alpha, \beta \in \Phi$. A subset of Φ is a π-system if and only if it is a basis of a root subsystem of Φ.

Definition 30. Let $\Gamma \subset \Phi$ be a π-system. Let $\Pi \subset \Gamma$ be a subset corresponding to a connected component of the Dynkin diagram of Γ. Let Ψ be the root subsystem of Φ spanned by Π, and let α_0 be its highest root. Let Π' be the set obtained from Π by erasing one element, and adding $-\alpha_0$. If the Dynkin diagram of Π' is different than the one of Π then we replace Π by Π' in Γ, obtaining a new π-system Γ', which is said to have been obtained from Γ by an **elementary transformation**.

Now we have the following procedure for classifying the $\mathfrak{h}^c$-regular semisimple subalgebras of $\mathfrak{g}^c$, up to G^c-conjugacy:

1. Let Δ be a basis of simple roots of Φ, and let P'' be the set of all π-systems obtainable from Δ by elementary transformations.

2. Let P' be the set of π-systems obtained from P'' by adding all subsets of each element of P''.

3. Let W denote the Weyl group of Φ. Remove all W-conjugate copies from P' to obtain the set P.

4. For each element Π in P construct the $\mathfrak{h}^c$-regular subalgebra of $\mathfrak{g}^c$ whose root system is spanned by Π.

5.10 Listing regular semisimple subalgebras

Throughout this section $\mathfrak{g}$ is a real semisimple Lie algebra with Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$, and Cartan involution θ. Also, by $\sigma : \mathfrak{g}^c \to \mathfrak{g}^c$ we denote the complex conjugation of $\mathfrak{g}^c$ with respect to $\mathfrak{g}$. By G we denote the adjoint group of $\mathfrak{g}$. Also, $\mathfrak{h}$ will be a θ-stable Cartan subalgebra of $\mathfrak{g}$.

Lemma 5.15. *Let $\mathfrak{a} \subset \mathfrak{g}$ be a semisimple subalgebra. Then*

1. *$C_\mathfrak{g}(\mathfrak{a}) = \mathfrak{s} \oplus \mathfrak{c}$ (direct sum of ideals), where $\mathfrak{s}$ is semisimple and $\mathfrak{c}$ is central and $\mathrm{ad}_\mathfrak{g} x$ is a semisimple linear transformation for all $x \in \mathfrak{c}$.*
2. *$N_\mathfrak{g}(\mathfrak{a}) = C_\mathfrak{g}(\mathfrak{a}) \oplus \mathfrak{a}$ (direct sum of ideals).*

Proof. The first statement is well-known, see for example [74], Proposition 20.5.13.

For the second statement, let $x \in N_\mathfrak{g}(\mathfrak{a})$. Then the restriction of $\mathrm{ad}_\mathfrak{g} x$ to $\mathfrak{a}$ is a derivation of $\mathfrak{a}$. Since $\mathfrak{a}$ is semisimple, all of its derivations are inner, so there is a $y \in \mathfrak{a}$ such that $\mathrm{ad}_\mathfrak{g} x|_\mathfrak{a} = \mathrm{ad}_\mathfrak{a} y$. So $x - y \in C_\mathfrak{g}(\mathfrak{a})$. Furthermore, it is obvious that $\mathfrak{a} \cap C_\mathfrak{g}(\mathfrak{a}) = 0$ and $[\mathfrak{a}, C_\mathfrak{g}(\mathfrak{a})] = 0$. So the second statement follows as well. □

Proposition 5.16. *Let $\mathfrak{a} \subset \mathfrak{g}$ be a semisimple $\mathfrak{h}$-regular subalgebra. Then $\mathfrak{a}$ is θ-stable.*

Proof. Let Φ be the root system of $\mathfrak{g}^c$ with respect to $\mathfrak{h}^c$. Let $\alpha \in \Phi$. As in Section 5.8 we write α^θ for $\alpha \circ \theta$ (note that $\theta = \theta^{-1}$). Then $\theta(\mathfrak{g}^c_\alpha) = \mathfrak{g}^c_{\alpha^\theta}$. Moreover, it is straightforward to show that $\sigma(\mathfrak{g}^c_\alpha) = \mathfrak{g}^c_{-\alpha^\theta}$. (Indeed, let $x_\alpha \in \mathfrak{g}^c_\alpha$, and $h \in \mathfrak{h} \cap \mathfrak{k}$, then $\mathrm{ad}_\mathfrak{g} h$ has purely imaginary eigenvalues, so that $[h, \sigma(x_\alpha)] = \sigma([h, x_\alpha]) = \overline{\alpha(h)}\sigma(x_\alpha) = -\alpha(h)\sigma(x_\alpha)$. Similarly, if $h \in \mathfrak{h} \cap \mathfrak{p}$ then $[h, \sigma(x_\alpha)] = \alpha(h)\sigma(x_\alpha)$; this implies that $x_\alpha \in \mathfrak{g}_{-\alpha^\theta}$.) Now $\mathfrak{a}^c$ is σ-stable, so that $\mathfrak{g}^c_{-\alpha^\theta} \subset \mathfrak{a}^c$. Furthermore, since $\mathfrak{a}^c$ is $\mathfrak{h}^c$-regular, its root system is a root subsystem of Φ, whence also $\mathfrak{g}^c_{\alpha^\theta} \subset \mathfrak{a}^c$. So $\mathfrak{a}^c$ is θ-stable. But $\mathfrak{a} = \{x \in \mathfrak{a}^c \mid \sigma(x) = x\}$. This implies that $\mathfrak{a}$ is θ-stable. □

Let $\mathfrak{a} \subset \mathfrak{g}$ be a $\mathfrak{h}$-regular semisimple subalgebra. By the previous proposition $\mathfrak{a}$ is θ-stable. Then also $N_\mathfrak{g}(\mathfrak{a})$ is θ-stable. By Lemma 5.15, $N_\mathfrak{g}(\mathfrak{a}) = \mathfrak{b} \oplus \mathfrak{c}$, where $\mathfrak{b}$ is semisimple and $\mathfrak{c}$ consists of semisimple elements. Moreover, $\mathfrak{b}$ is the derived subalgebra, and $\mathfrak{c}$ is the centre of $N_\mathfrak{g}(\mathfrak{a})$. So both are θ-stable. In particular, $\mathfrak{b} \cap \mathfrak{k} \oplus \mathfrak{b} \cap \mathfrak{p}$ is a Cartan decomposition of $\mathfrak{b}$. Let $\tilde{\mathfrak{h}}$ be a maximally noncompact Cartan subalgebra of $\mathfrak{b}$. Then $\tilde{\mathfrak{h}} \oplus \mathfrak{c}$ is a maximally noncompact Cartan subalgebra of $N_\mathfrak{g}(\mathfrak{a})$, and all maximally noncompact Cartan subalgebras of $N_\mathfrak{g}(\mathfrak{h})$ arise in this manner. Note that also $\mathfrak{h}$ is a Cartan subalgebra of $N_\mathfrak{g}(\mathfrak{a})$.

Definition 31. We say that $\mathfrak{a}$ is **strongly $\mathfrak{h}$-regular** if $\mathfrak{h}$ is a maximally noncompact Cartan subalgebra of $N_\mathfrak{g}(\mathfrak{a})$.

Next algorithm checks whether a given $\mathfrak{h}$-regular semisimple subalgebra is strongly $\mathfrak{h}$-regular.

Algorithm 3
$\mathfrak{a}$ is a $\mathfrak{h}$-regular semisimple subalgebra of $\mathfrak{g}$, where $\mathfrak{h}$ is a θ-stable Cartan subalgebra of $\mathfrak{g}$; we return **True** if $\mathfrak{a}$ is strongly $\mathfrak{h}$-regular, **False** otherwise.

- Compute $\mathfrak{v} = \mathfrak{h} \cap \mathfrak{p}$
- If $C_\mathfrak{g}(\mathfrak{v}) \cap N_\mathfrak{g}(\mathfrak{h}) \cap \mathfrak{p} = \mathfrak{v}$ return then **True**
- else return **False**

Lemma 5.17. *Algorithm 3 is correct.*

Proof. By [60], Proposition 6.47, see also the remarks on [60], page 386, we have that $\mathfrak{h}$ is a maximally noncompact Cartan subalgebra of $N_{\mathfrak{g}}(\mathfrak{a})$ if and only if $\mathfrak{v} = \mathfrak{h} \cap \mathfrak{p}$ is a maximal abelian subspace of $N_{\mathfrak{g}}(\mathfrak{a}) \cap \mathfrak{p}$. The latter is the case if and only if the intersection of the centralizer of $\mathfrak{v}$ and $N_{\mathfrak{g}}(\mathfrak{a}) \cap \mathfrak{p}$ is exactly $\mathfrak{v}$. □

Lemma 5.18. *Let $\mathfrak{a}$, $\mathfrak{a}'$ be strongly $\mathfrak{h}$-regular semisimple subalgebras of $\mathfrak{g}$. Then $\mathfrak{a}$ and $\mathfrak{a}'$ are conjugate under G if and only if they are conjugate under $N_G(\mathfrak{h})$.*

Proof. Only one implication requires proof. Let $g \in G$ be such that $g(\mathfrak{a}) = \mathfrak{a}'$. Then $g(\mathfrak{h})$ is a maximally noncompact Cartan subalgebra of $N_{\mathfrak{g}}(\mathfrak{a}')$. So it is conjugate to $\mathfrak{h}$ under the adjoint group of $N_{\mathfrak{g}}(\mathfrak{a}')$, which is $N_G(\mathfrak{a}')$. In other words, there is a $g' \in N_G(\mathfrak{a}')$ such that $g'g(\mathfrak{h}) = \mathfrak{h}$. But then $g'g \in N_G(\mathfrak{h})$ and $g'g(\mathfrak{a}) = \mathfrak{a}'$. □

Let Φ be the root system of $\mathfrak{g}^c$ relative to $\mathfrak{h}^c$. Let $\mathfrak{a} \subset \mathfrak{g}$ be a $\mathfrak{h}$-regular semisimple subalgebra. Then the set

$$\Psi(\mathfrak{a}) = \{\alpha \in \Phi \mid \overset{c}{\underset{\alpha}{\mathfrak{g}}} \subset \mathfrak{a}^c\}$$

is a root subsystem of Φ.

Theorem 5.19. *Let W denote the Weyl group of Φ. Let $W(\mathfrak{h}) \subset W$ be the real Weyl group of $\mathfrak{h}$. Let $\mathfrak{a}, \mathfrak{a}'$ be strongly $\mathfrak{h}$-regular semisimple subalgebras of $\mathfrak{g}$. Then $\mathfrak{a}, \mathfrak{a}'$ are G-conjugate if and only if $\Psi(\mathfrak{a})$ and $\Psi(\mathfrak{a}')$ are $W(\mathfrak{h})$-conjugate.*

Proof. Suppose that the subalgebras are G-conjugate. By Lemma 5.18, there is a $g \in N_G(\mathfrak{h})$ such that $g(\mathfrak{a}) = \mathfrak{a}'$. Let $\alpha \in \Psi(\mathfrak{a})$. Then $g(\mathfrak{g}^c_\alpha) = \mathfrak{g}^c_{\alpha^{g^{-1}}}$. So $\alpha^{g^{-1}} \in \Psi(\mathfrak{a}')$. But as shown in Section 5.8, the map $\alpha \mapsto \alpha^{g^{-1}}$ lies in $W(\mathfrak{h})$.
Conversely, suppose that there is a $w \in W(\mathfrak{h})$ such that $w(\Psi(\mathfrak{a})) = \Psi(\mathfrak{a}')$. Let $g \in N_G(\mathfrak{h})$ be such that g projects to w under $N_G(\mathfrak{h}) \to N_G(\mathfrak{h})/Z_G(\mathfrak{h}) \cong W(\mathfrak{h})$. Then $w(\alpha) = \alpha^{g^{-1}}$. It follows that $g(\mathfrak{a}) = \mathfrak{a}'$. □

This theorem yields a straightforward algorithm for checking whether two given strongly $\mathfrak{h}$-regular semisimple subalgebras, $\mathfrak{a}, \mathfrak{a}'$, are G-conjugate: run over all $w \in W(\mathfrak{h})$ and check whether $w(\Psi(\mathfrak{a})) = \Psi(\mathfrak{a}')$.
Now we are ready to state the main algorithm of this paper. We just need one more piece of notation. Again, let W be the Weyl group of Φ. Let $w \in W$. Let $\mathfrak{a}^c$ be a $\mathfrak{h}^c$-regular semisimple subalgebra of $\mathfrak{g}^c$. Then $w \cdot \mathfrak{a}^c$ denotes the $\mathfrak{h}^c$-regular semisimple subalgebra of $\mathfrak{g}^c$ whose root system is $w(\Psi(\mathfrak{a}^c))$.

Algorithm 4
$\mathfrak{h}$ is a θ-stable Cartan subalgebra of $\mathfrak{g}$; we return a list of strongly $\mathfrak{h}$-regular semisimple subalgebras of $\mathfrak{g}$, such that each such subalgebra of $\mathfrak{g}$ is G-conjugate to exactly one element of the list.

1. Compute the root system Φ of $\mathfrak{g}^c$ with respecto to $\mathfrak{h}^c$, and generators of its Weyl group W
2. Use Dynkin's algorithm to obtain a list R of $\mathfrak{h}^c$-regular semisimple subalgebras of $\mathfrak{g}^c$, up to G^c-conjugacy
3. Compute the real Weyl group $W(\mathfrak{h}) \subset W$
4. Compute a set $w_1, \ldots, w_s$ of representatives of the right cosets of $W(\mathfrak{h})$ in W
5. Set $L = \emptyset$;
6. For $\mathfrak{a}^c \in R$ do:
7. $\quad L_0 := \emptyset$
8. $\quad$ For $1 \leq i \leq s$ do
9. $\quad\quad$ Set $\tilde{\mathfrak{a}}^c := w_i \cdot \mathfrak{a}^c$
10. $\quad\quad$ If $\tilde{\mathfrak{a}}^c$ is σ-stable then
11. $\quad\quad\quad$ Set $\tilde{\mathfrak{a}} := \{x \in \tilde{\mathfrak{a}}^c \mid \sigma(x) = x\}$
12. $\quad\quad\quad$ if $\tilde{\mathfrak{a}}$ is strongly $\mathfrak{h}$-regular then
13. $\quad\quad\quad\quad$ Add $\tilde{\mathfrak{a}}$ to L_0
14. $\quad$ Get rid of G-conjugate copies in L_0
15. Set $L := L \cup L_0$
16. Return L

Proposition 5.20. *Algorithm 4 is correct.*

Proof. Let L denote the output. Then L contains no G-conjugate subalgebras. Indeed, if $\mathfrak{b}, \mathfrak{b}' \in L$ are G-conjugate, then $\mathfrak{b}^c$, $(\mathfrak{b}')^c$ are G^c-conjugate to the same $\mathfrak{a}^c$ in R. So they have both been added when considering $\mathfrak{a}^c$ in the loop starting on line 6. But then they cannot both be in L since on line 14 one of them is erased.
Let $\mathfrak{a}'$ be a strongly $\mathfrak{h}$-regular semisimple subalgebra of $\mathfrak{g}$. Then $(\mathfrak{a}')^c$ is G^c-conjugate to an $\mathfrak{a}^c \in R$. So there is a $w \in W$ such that $w \cdot \mathfrak{a}^c = (\mathfrak{a}')^c$. There is a w_i and $u \in W(\mathfrak{h})$ such that $w = uw_i$. So $w_i \cdot \mathfrak{a}^c$ is $W(\mathfrak{h})$-conjugate to $(\mathfrak{a}')^c$. At some point, in the iteration $\mathfrak{a}^c$ (loop on line 6) and i (loop on line 8) are considered. So $\tilde{\mathfrak{a}}^c = w_i \cdot \mathfrak{a}^c$ is constructed. It is σ-stable as $\tilde{\mathfrak{a}}^c$ is $W(\mathfrak{h})$-conjugate to $(\mathfrak{a}')^c$, which is σ-stable. So the real subalgebra $\tilde{\mathfrak{a}}$ is constructed on line 11. Now $\tilde{\mathfrak{a}}$ is $W(\mathfrak{h})$-conjugate to $\mathfrak{a}'$, so $\tilde{\mathfrak{a}}$ is strongly $\mathfrak{h}$-regular. Therefore, on line 13, $\tilde{\mathfrak{a}}$ is added to the list. Finally, by Theorem 5.19, $\tilde{\mathfrak{a}}$ is G-conjugate to $\mathfrak{a}'$. The conclusion is that every strongly $\mathfrak{h}$-regular semisimple subalgebra of $\mathfrak{g}$ is G-conjugate to an element of L. □

Proposition 5.21. *Let $\mathfrak{h}_1, \ldots, \mathfrak{h}_t$ be the list of θ-stable Cartan subalgebras of $\mathfrak{g}$, up to G-conjugacy. Let L_i be the output of Algorithm 4 with input $\mathfrak{h}_i$. Then the union L of the L_i is the list of regular semisimple subalgebras of $\mathfrak{g}$, up to G-conjugacy.*

Proof. Let $\mathfrak{a}$ be a regular semisimple subalgebra of $\mathfrak{g}$, and let $\tilde{\mathfrak{h}}$ be a maximally non-compact Cartan subalgebra of $N_{\mathfrak{g}}(\mathfrak{a})$. Then there is a $g \in G$ and an index i, such that $g(\tilde{\mathfrak{h}}) = \mathfrak{h}_i$. So $g(\mathfrak{a})$ is $\mathfrak{h}_i$-regular. Since $\tilde{\mathfrak{h}}$ is maximally noncompact in $N_{\mathfrak{g}}(\mathfrak{a})$ we get that $g(\mathfrak{a})$ is strongly $\mathfrak{h}_i$-regular. It cannot be strongly $\mathfrak{h}_j$-regular as well (if $i \neq j$), as that would imply that $\mathfrak{h}_i$ and $\mathfrak{h}_j$ are G-conjugate.
From this we conclude that L contains a G-conjugate of every regular semisimple subalgebra $\mathfrak{a}$ of $\mathfrak{g}$, and moreover, it does not contain two subalgebras that are G-conjugate, by Proposition 5.20. □

5.11 Tables of regular subalgebras

Let $\mathfrak{h}$ be a θ-stable Cartan subalgebra of the semisimple real Lie algebra $\mathfrak{g}$. Let Φ be the root system of $\mathfrak{g}^c$ with respect to $\mathfrak{h}^c$. Then for $\alpha \in \Phi$ there is a $\beta \in \Phi$ such that $\theta(\mathfrak{g}^c_\alpha) = \mathfrak{g}^c_\beta$. We write $\beta = \alpha^\theta$. We can now state the following definitions.

Definition 32. A root α is said to be:

- **real** if $\alpha^\theta = -\alpha$. (This means that $\alpha(\mathfrak{h} \cap \mathfrak{k}) = 0$.)
- **imaginary** if $\alpha^\theta = \alpha$. (This means that $\alpha(\mathfrak{h} \cap \mathfrak{p}) = 0$.)
- **compact imaginary** if it is imaginary and θ acts as the identity on $\mathfrak{g}^c_\alpha$. (So that $\mathfrak{g}^c_\alpha \subset \mathfrak{k}$.)

The sets of real, imaginary and compact imaginary roots each form a root subsystem of Φ. In the following we list these root systems for each Cartan subalgebra of a given real simple Lie algebra. We also list the dimensions of $\mathfrak{h} \cap \mathfrak{k}$ and $\mathfrak{h} \cap \mathfrak{p}$.

5.11.1 G

The real simple Lie algebra of type G has four Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	G_2			0, 2
$\mathfrak{h}_2$	A_1	A_1		1, 1
$\mathfrak{h}_3$	A_1	A_1		1, 1
$\mathfrak{h}_4$		G_2	$A_1 \oplus A_1$	2, 0

The corresponding regular subalgebras are given in Tables 11, 12 and 13.

5.11.2 $\mathfrak{so}^*_8$

The simple real Lie algebra $\mathfrak{so}^*_8$ has three Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	$A_1 \oplus A_1$	$A_1 \oplus A_1 \oplus A_1$	$A_1 \oplus A_1$	2, 2
$\mathfrak{h}_2$	A_1	$A_1 \oplus A_1 \oplus A_1$	$A_1 \oplus A_1$	3, 1
$\mathfrak{h}_3$		D_4	A_3	4, 0

The corresponding regular subalgebras are given in Tables 14, 15 and 16

5.11.3 $\mathfrak{so}_{4,4}$

The simple real Lie algebra $\mathfrak{so}_{4,4}$ has seven Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	D_4			0, 4
$\mathfrak{h}_2$	$A_1 \oplus A_1 \oplus A_1$	A_1		1, 3
$\mathfrak{h}_3$	$A_1 \oplus A_1$	$A_1 \oplus A_1$		2, 2
$\mathfrak{h}_4$	$A_1 \oplus A_1$	$A_1 \oplus A_1$		2, 2
$\mathfrak{h}_5$	$A_1 \oplus A_1$	$A_1 \oplus A_1$		2, 2
$\mathfrak{h}_6$	A_1	$A_1 \oplus A_1 \oplus A_1$		3, 1
$\mathfrak{h}_7$		D_4	$A_1 \oplus A_1 \oplus A_1 \oplus A_1$	4, 0

The corresponding regular subalgebras are given in Tables 17, 18, 19, 20, 21, 22 and 23.

5.11.4 $\mathfrak{so}_{3,5}$

The simple real Lie algebra $\mathfrak{so}_{3,5}$ has three Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	A_3			1, 3
$\mathfrak{h}_2$	A_1	A_1		2, 2
$\mathfrak{h}_3$		A_3	$A_1 \oplus A_1$	3, 1

The corresponding regular subalgebras are given in Tables 24, 25 and 26

5.11.5 $\mathfrak{so}_{1,7}$

The simple real Lie algebra $\mathfrak{so}_{1,7}$ has one Cartan subalgebra.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$		A_3	A_3	3, 1

The corresponding regular subalgebras are given in Table 27.

5.11.6 FII

The simple real Lie algebra of type FII has two Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	A_1	B_3	B_3	3, 1
$\mathfrak{h}_2$		F_4	B_4	4, 0

The corresponding regular subalgebras are given in Tables 28 and 29.

5.11.7 EI

The simple real Lie algebra of type EI has five Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	E_6			0, 6
$\mathfrak{h}_2$	A_5	A_1		1, 5
$\mathfrak{h}_3$	A_3	$A_1 \oplus A_1$		2, 4
$\mathfrak{h}_4$	A_1	$A_1 \oplus A_1 \oplus A_1$		3, 3
$\mathfrak{h}_5$		D_4	$A_1 \oplus A_1 \oplus A_1 \oplus A_1$	4, 2

The corresponding regular subalgebras are given in Tables 30, 31, 32, 33 and 34.

5.11.8 EII

The simple real Lie algebra of type EII has five Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	D_4			2, 4
$\mathfrak{h}_2$	$A_1 \oplus A_1 \oplus A_1$	A_1		3, 3
$\mathfrak{h}_3$	$A_1 \oplus A_1$	A_3	$A_1 \oplus A_1$	4, 2
$\mathfrak{h}_4$	A_1	A_5	$A_2 \oplus A_2$	5, 1
$\mathfrak{h}_5$		E_6	$A_1 \oplus A_5$	6, 0

The corresponding regular subalgebras are given in Tables 38, 39 and 40.

5.11.9 EIII

The simple real Lie algebra of type EIII has three Cartan subalgebras.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$	$A_1 \oplus A_1$	A_3	A_3	4, 2
$\mathfrak{h}_2$	A_1	A_5	A_4	5, 1
$\mathfrak{h}_3$		E_6	D_5	6, 0

The corresponding regular subalgebras are given in Table 35, 36 and 37.

5.11.10 EIV

The simple real Lie algebra of type EIV has one Cartan subalgebra.

CSA	real	imaginary	compact	decomposition
$\mathfrak{h}_1$		D_4	D_4	4, 2

The corresponding regular subalgebras are given in Tables 41.

Type	Real Subalgebra	Centralizer
A_1^3	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R})$
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R})$
A_2^1	$\mathfrak{sl}_3(\mathbb{R})$	T_0
$A_1^1 \oplus A_1^3$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$T_{0,0}$

Table 11: Strongly $\mathfrak{h}_1$-regular subalgebras of G

Type	Real Subalgebra	Centralizer
A_2^1	$\mathfrak{su}_{1,2}$	$T_{0,0}$

Table 12: Strongly $\mathfrak{h}_2$-regular subalgebras of G

Type	Real Subalgebra	Centralizer
A_1^3	$\mathfrak{su}_2$	$\mathfrak{su}_2$
A_1^1	$\mathfrak{su}_2$	$\mathfrak{su}_2$
A_2^1	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,0}$

Table 13: Strongly $\mathfrak{h}_4$-regular subalgebras of G

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$
	$\mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R})$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$
A_3^1	$\mathfrak{su}_{2,2}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{H})$	$T_{0,1}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{C})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,0}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,0}$

Table 14: Strongly $\mathfrak{h}_1$-regular subalgebras of $\mathfrak{so}_8^*$

Type	Real Subalgebra	Centralizer
A_2^1	$\mathfrak{su}_{1,2}$	$T_{2,0}$
A_3^1	$\mathfrak{su}_{1,3}$	$T_{1,0}$
A_3^1	$\mathfrak{su}_{1,3}$	$T_{1,0}$

Table 15: Strongly $\mathfrak{h}_2$-regular subalgebras of $\mathfrak{so}_8^*$

Type	Real Subalgebra	Centralizer
A_2^1	$\mathfrak{su}_3$	$T_{2,0}$
A_3^1	$\mathfrak{su}_4$	$T_{1,0}$

Table 16: Strongly $\mathfrak{h}_3$-regular subalgebras of $\mathfrak{so}_8^*$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
A_2^1	$\mathfrak{sl}_3(\mathbb{R})$	$T_{0,2}$
A_3^1	$\mathfrak{sl}_4(\mathbb{R})$	$T_{0,1}$
A_3^1	$\mathfrak{sl}_4(\mathbb{R})$	$T_{0,1}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R})$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
A_3^1	$\mathfrak{sl}_4(\mathbb{R})$	$T_{0,1}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$T_{0,0}$

Table 17: Strongly $\mathfrak{h}_1$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})2$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R})$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$

Table 18: Strongly $\mathfrak{h}_2$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_3^1	$\mathfrak{su}_{2,2}$	$T_{1,0}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{C})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,0}$

Table 19: Strongly $\mathfrak{h}_3$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_3^1	$\mathfrak{su}_{2,2}$	$T_{1,0}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{C})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,0}$

Table 20: Strongly $\mathfrak{h}_4$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_3^1	$\mathfrak{sl}_{2,2}$	$T_{1,0}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{C})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,0}$

Table 21: Strongly $\mathfrak{h}_5$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_2^1	$\mathfrak{sl}_{1,2}$	$T_{2,0}$

Table 22: Strongly $\mathfrak{h}_6$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,0}$

Table 23: Strongly $\mathfrak{h}_7$-regular subalgebras of $\mathfrak{so}_{4,4}$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{C})$
A_2^1	$\mathfrak{sl}_3(\mathbb{R})$	$T_{1,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{R})$
A_3^1	$\mathfrak{sl}_4(\mathbb{R})$ $\mathfrak{su}_{2,2}$	$T_{1,0}$ $T_{0,1}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$ $\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{C})$ $\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,0}$

Table 24: Strongly $\mathfrak{h}_1$-regular subalgebras of $\mathfrak{so}_{3,5}$

Type	Real Subalgebra	Centralizer
A_2^1	$\mathfrak{su}_{1,2}$	$T_{1,1}$

Table 25: Strongly $\mathfrak{h}_2$-regular subalgebras of $\mathfrak{so}_{3,5}$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2$
A_3^1	$\mathfrak{sl}_2(\mathbb{H})$	$T_{1,0}$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{C})$
	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,0}$

Table 26: Strongly $\mathfrak{h}_3$-regular subalgebras of $\mathfrak{so}_{3,5}$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$
A_2^1	$\mathfrak{su}_3$	$T_{1,1}$
A_3^1	$\mathfrak{su}_4$	$T_{0,1}$
	$\mathfrak{sl}_2(\mathbb{H})$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{C})$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,0}$

Table 27: Strongly $\mathfrak{h}_1$-regular subalgebras of $\mathfrak{so}_{1,7}$

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{sp}_{1,2}$
A_2^1	$\mathfrak{su}_3$	$\mathfrak{su}_{1,2}$
B_3^1	$\mathfrak{so}_7$	$T_{0,1}$
	$\mathfrak{so}_{6,1}$	$T_{1,0}$
$A_1^2 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3$	$T_{1,0}$
$A_1^2 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{0,1}$
	$\mathfrak{sl}_2\mathbb{R} \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^2 \oplus A_2^1$	$\mathfrak{sl}_{1,2} \oplus \mathfrak{su}_2$	$T_{1,0}$
B_2^1	$\mathfrak{so}_5$	$\mathfrak{sl}_2(\mathbb{C})$
	$\mathfrak{so}_{1,4}$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
C_3^1	$\mathfrak{sp}_{1,2}$	$\mathfrak{su}_2$
A_1^2	$\mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{H})$
	$\mathfrak{sl}_2\mathbb{R}$	$\mathfrak{su}_4$
A_2^2	$\mathfrak{su}_{1,2}$	$\mathfrak{su}_3$
$A_1^1 \oplus C_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{sp}_{1,2}$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^2$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$	$T_{1,0}$
$A_1^1 \oplus A_1^2 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,1}$
$A_1^2 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{1,0}$
$A_1^1 \oplus B_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{so}_{1,4}$	$\mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{so}_{1,4}$
	$\mathfrak{sl}_2\mathbb{C}$	$\mathfrak{so}_5$
$A_2^2 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_3$	$T_{0,0}$
$A_1^1 \oplus A_3^2$	$\mathfrak{su}_2 \oplus \mathfrak{sl}_2(\mathbb{H})$	$T_{0,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_4$	$T_{0,0}$
A_3^1	$\mathfrak{sl}_2(\mathbb{H})$	$\mathfrak{su}_2$
	$\mathfrak{su}_4$	$\mathfrak{sl}_2\mathbb{R}$
B_4^1	$\mathfrak{so}_{1,8}$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus B_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{so}_{1,4}$	$T_{0,0}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{so}_5$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{su}_2$
D_4^1	$\mathfrak{so}_{1,7}$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,0}$

Table 28: Strongly $\mathfrak{h}_1$-regular subalgebras of FII

Type	Real Subalgebra	Centralizer
B_3^1	$\mathfrak{so}_7$	$T_{1,0}$
$A_1^1 \oplus A_2^2$	$\mathfrak{su}_2 \oplus \mathfrak{su}_3$	$T_{1,0}$
$A_1^2 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{1,0}$
B_2^1	$\mathfrak{so}_5$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$
A_1^2	$\mathfrak{su}_2$	$\mathfrak{su}_4$
$A_1^1 \oplus A_1^2 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{1,0}$
$A_1^1 \oplus B_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{so}_5$	$\mathfrak{su}_2$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{so}_{1,4}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{so}_5$
$A_1^1 \oplus A_3^2$	$\mathfrak{su}_2 \oplus \mathfrak{su}_4$	$T_{0,0}$
A_3^1	$\mathfrak{su}_4$	$\mathfrak{su}_2$
	$\mathfrak{su}_4$	$\mathfrak{sl}_2\mathbb{R}$
B_4^1	$\mathfrak{so}_9$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus B_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{so}_5$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2$
D_4^1	$\mathfrak{so}_8$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,0}$

Table 29: Strongly $\mathfrak{h}_2$-regular subalgebras of FII

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_6(\mathbb{R})$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_4(\mathbb{R}) \oplus T_{0,1}$
$A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R})$	$\mathfrak{sl}_3(\mathbb{R}) \oplus T_{0,1}$
A_4^1	$\mathfrak{sl}_5(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{0,1}$
D_5^1	$\mathfrak{so}_{5,5}$	$T_{0,1}$
$A_1^1 \oplus A_4^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_5(\mathbb{R})$	$T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R})$	$T_{0,2}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R})$	$T_{0,1}$
$A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_4(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{0,2}$
A_2^1	$\mathfrak{sl}_3(\mathbb{R})$	$\mathfrak{sl}_3(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R})$
A_3^1	$\mathfrak{sl}_4(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus T_{0,1}$
A_5^1	$\mathfrak{sl}_6(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R})$
$A_2^1 \oplus A_2^1$	$\mathfrak{sl}_3(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R})$	$\mathfrak{sl}_3(\mathbb{R})$
D_4^1	$\mathfrak{so}_{4,4}$	$T_{0,2}$
$A_1^1 \oplus A_5^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_6(\mathbb{R})$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_4(\mathbb{R})$	$T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$T_{0,2}$
$A_2^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_3(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{R})$	$T_{0,0}$

Table 30: Strongly $\mathfrak{h}_1$-regular subalgebras of EI

Type	Real Subalgebra	Centralizer
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{su}_{2,2} \oplus T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,1}$
A_3^1	$\mathfrak{su}_{2,2}$	$\mathfrak{sl}_2(\mathbb{C}) \oplus T_{0,1}$
D_4^1	$\mathfrak{so}_{1,7}$	$T_{1,1}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_{2,2}$	$T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$ $\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{0,2}$ $T_{1,1}$

Table 31: Strongly $\mathfrak{h}_3$-regular subalgebras of EI

Type	Real Subalgebra	Centralizer
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{1,1}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{C})$	$T_{1,0}$
A_2^1	$\mathfrak{su}_{1,2}$	$\mathfrak{sl}_3(\mathbb{C})$
$A_1^2 \oplus A_1^2$	$\mathfrak{sl}_3(\mathbb{C})$	$\mathfrak{su}_{1,2}$
$A_2^2 \oplus A_2^2 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{sl}_3(\mathbb{C})$	$T_{0,0}$

Table 32: Strongly $\mathfrak{h}_4$-regular subalgebras of EI

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{su}_{2,4}$
	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{su}_{1,5}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{H}) \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_{1,3} \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_{2,2} \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{su}_4 \oplus T_{1,0}$
$A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_3 \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_{1,2} \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3$	$\mathfrak{su}_{1,2} \oplus T_{1,0}$
A_4^1	$\mathfrak{su}_{2,3}$	$\mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_{1,4}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
D_5^1	$\mathfrak{so}_{10}^*$	$T_{1,0}$
	$\mathfrak{so}_{2,8}$	$T_{1,0}$
$A_1^1 \oplus A_4^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{2,3}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,4}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3$	$T_{2,0}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3 \oplus \mathfrak{su}_{1,2}$	$T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$T_{1,0}$
$A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{2,2}$	$\mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,3}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_4$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,3}$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{1,1}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{2,0}$
A_2^1	$\mathfrak{su}_{1,2}$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_3$
	$\mathfrak{su}_3$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1.2}$
A_3^1	$\mathfrak{su}_{1,3}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{H})$	$\mathfrak{sl}_2(\mathbb{C}) \oplus T_{1,0}$
	$\mathfrak{su}_{2,2}$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_4$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
A_5^1	$\mathfrak{su}_{1,5}$	$\mathfrak{sl}_2(\mathbb{R})$
	$\mathfrak{su}_{2,4}$	$\mathfrak{su}_2$
$A_2^1 \oplus A_2^1$	$\mathfrak{su}_3 \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_{1,2}$
	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_3$
D_4^1	$\mathfrak{so}_{1,7}$	$T_{1,1}$
	$\mathfrak{so}_8^*$	$T_{2,0}$
$A_1^1 \oplus A_5^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,5}$	$T_{0,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_{2,4}$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{1,3}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{H})$	$T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{2,2}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_4$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{1,1}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{2,0}$
$A_2^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_3 \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$T_{0,0}$

Table 33: Strongly $\mathfrak{h}_1$-regular subalgebras of EIII

Type	Real Subalgebra	Centralizer
$A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_3$	$\mathfrak{su}_{1,2} \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_3 \oplus T_{1,0}$
A_4^1	$\mathfrak{su}_5$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
	$\mathfrak{su}_{1,4}$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_4^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,4}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_5$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$T_{2,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3$	$T_{2,0}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_3 \oplus \mathfrak{su}_{1,2}$	$T_{1,0}$

Table 34: Strongly $\mathfrak{h}_2$-regular subalgebras of EIII

Type	Real Subalgebra	Centralizer
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_4 \oplus T_{1,0}$
D_5^1	$\mathfrak{so}_{10}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_3$	$T_{2,0}$
$A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_4$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{2,0}$
A_3^1	$\mathfrak{su}_4$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus T_{1,0}$
D_4^1	$\mathfrak{so}_8$	$T_{2,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_4$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{2,0}$

Table 35: Strongly $\mathfrak{h}_3$-regular subalgebras of EIII

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{su}_{3,3}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{su}_{2,2} \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_4(\mathbb{R}) \oplus T_{1,0}$
D_5^1	$\mathfrak{so}_{4,6}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_3(\mathbb{R})$	$T_{1,1}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{C})$	$T_{0,1}$
$A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{2,2}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,1}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{2,0}$
A_2^1	$\mathfrak{sl}_3(\mathbb{R})$	$\mathfrak{sl}_3(\mathbb{C})$
A_3^1	$\mathfrak{su}_{2,2}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
	$\mathfrak{sl}_4(\mathbb{R})$	$\mathfrak{sl}_2(\mathbb{C}) \oplus T_{1,0}$
A_5^1	$\mathfrak{su}_{3,3}$	$\mathfrak{sl}_2(\mathbb{R})$
$A_2^1 \oplus A_2^1$	$\mathfrak{sl}_3(\mathbb{C})$	$\mathfrak{sl}_3(\mathbb{R})$
D_4^1	$\mathfrak{so}_{3,5}$	$T_{1,1}$
	$\mathfrak{so}_{4,4}$	$T_{2,0}$
$A_1^1 \oplus A_5^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{3,3}$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{2,2}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_4(\mathbb{R})$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$T_{1,1}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R})$	$T_{2,0}$
$A_2^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_3(\mathbb{R}) \oplus \mathfrak{sl}_3(\mathbb{C})$	$T_{0,0}$

Table 36: Strongly $\mathfrak{h}_1$-regular subalgebras of EII

Type	Real Subalgebra	Centralizer
$A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_{1,2} \oplus T_{1,0}$
A_4^1	$\mathfrak{su}_{2,3}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
$A_1^1 \oplus A_4^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{2,3}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,2}$	$T_{2,0}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$T_{1,0}$
A_2^1	$\mathfrak{su}_{1,2}$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$
$A_2^1 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_{1,2}$
$A_2^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$T_{0,0}$

Table 37: Strongly $\mathfrak{h}_2$-regular subalgebras of EII

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{su}_{2,4}$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{sl}_2(\mathbb{H}) \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_{2,2} \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_{1,3} \oplus T_{1,0}$
$A_1^1 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_2$	$\mathfrak{su}_{1,2} \oplus T_{1,0}$
A_4^1	$\mathfrak{su}_{2,3}$	$\mathfrak{su}_2 \oplus T_{1,0}$
D_5^1	$\mathfrak{so}_{10}^*$	$T_{1,0}$
$A_1^1 \oplus A_4^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{2,3}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_2$	$T_{2,0}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_{1,2}$	$T_{1,0}$
$A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{2,2}$	$\mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,3}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_{1,3}$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{su}_2 \oplus T_{1,1}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{R}) \oplus T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{2,0}$
A_3^1	$\mathfrak{su}_{2,2}$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_{1,3}$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{H})$	$\mathfrak{sl}_2(\mathbb{C}) \oplus T_{1,0}$
A_5^1	$\mathfrak{su}_{2,4}$	$\mathfrak{su}_2$
D_4^1	$\mathfrak{so}_8^*$	$T_{2,0}$
$A_1^1 \oplus A_5^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{2,4}$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{H})$	$T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{2,2}$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{1,3}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{1,1}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$	$T_{2,0}$

Table 38: Strongly $\mathfrak{h}_3$-regular subalgebras of EII

Type	Real Subalgebra	Centralizer
$A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$\mathfrak{su}_3 \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_3$	$\mathfrak{su}_{1,2} \oplus T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3$	$\mathfrak{su}_3 \oplus T_{1,0}$
A_4^1	$\mathfrak{su}_{1,4}$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_4^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,4}$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$T_{2,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_3$	$T_{2,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_{1,2}$	$T_{2,0}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_{1,2} \oplus \mathfrak{su}_3$	$T_{1,0}$
	$\mathfrak{sl}_2(\mathbb{R}) \oplus \mathfrak{su}_3 \oplus \mathfrak{su}_3$	$T_{1,0}$
A_2^1	$\mathfrak{su}_{1,2}$	$\mathfrak{su}_3 \oplus \mathfrak{su}_3$
	$\mathfrak{su}_3$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_3$
$A_2^1 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_3$	$\mathfrak{su}_3$
	$\mathfrak{su}_3 \oplus \mathfrak{su}_3$	$\mathfrak{su}_{1,2}$
$A_2^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_{1,2} \oplus \mathfrak{su}_3 \oplus \mathfrak{su}_3$	$T_{0,0}$

Table 39: Strongly $\mathfrak{h}_4$-regular subalgebras of EII

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{su}_6$
$A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_4 \oplus T_{1,0}$
$A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_3$	$\mathfrak{su}_3 \oplus T_{1,0}$
A_4^1	$\mathfrak{su}_5$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_4^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_5$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_3$	$T_{2,0}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_3 \oplus \mathfrak{su}_3$	$T_{1,0}$
$A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_4$	$\mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_4$	$\mathfrak{su}_2 \oplus T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{1,0}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{1,0}$
A_3^1	$\mathfrak{su}_4$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus T_{1,0}$
A_5^1	$\mathfrak{su}_6$	$\mathfrak{su}_2$
$A_1^1 \oplus A_5^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_6$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_4$	$T_{1,0}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{2,0}$

Table 40: Strongly $\mathfrak{h}_5$-regular subalgebras of EII

Type	Real Subalgebra	Centralizer
A_1^1	$\mathfrak{su}_2$	$\mathfrak{sl}_3(\mathbb{H})$
$A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C})$	$\mathfrak{su}_4 \oplus T_{0,1}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{sl}_2(\mathbb{H}) \oplus T_{0,1}$
D_5^1	$\mathfrak{so}_{1,9}$	$T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_2^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_3$	$T_{1,1}$
$A_1^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_2 \oplus \mathfrak{sl}_3(\mathbb{C})$	$T_{1,0}$
$A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{sl}_2(\mathbb{H})$	$\mathfrak{su}_2 \oplus T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{1,1}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$\mathfrak{su}_2 \oplus T_{0,2}$
A_2^1	$\mathfrak{su}_3$	$\mathfrak{sl}_3(\mathbb{C})$
A_3^1	$\mathfrak{sl}_2(\mathbb{H})$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus T_{0,1}$
	$\mathfrak{su}_4$	$\mathfrak{sl}_2(\mathbb{C}) \oplus T_{0,1}$
A_5^1	$\mathfrak{sl}_3(\mathbb{H})$	$\mathfrak{su}_2$
$A_2^1 \oplus A_2^1$	$\mathfrak{sl}_3(\mathbb{C})$	$\mathfrak{su}_3$
D_4^1	$\mathfrak{so}_{1,7}$	$T_{1,1}$
	$\mathfrak{so}_8$	$T_{0,2}$
$A_1^1 \oplus A_5^1$	$\mathfrak{su}_2 \oplus \mathfrak{sl}_3(\mathbb{H})$	$T_{0,0}$
$A_1^1 \oplus A_1^1 \oplus A_3^1$	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{sl}_2(\mathbb{H})$	$T_{0,1}$
	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_4$	$T_{0,1}$
$A_1^1 \oplus A_1^1 \oplus A_1^1 \oplus A_1^1$	$\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{1,1}$
	$\mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2 \oplus \mathfrak{su}_2$	$T_{0,2}$
$A_2^1 \oplus A_2^1 \oplus A_2^1$	$\mathfrak{su}_3 \oplus \mathfrak{sl}_3(\mathbb{C})$	$T_{0,0}$

Table 41: Strongly $\mathfrak{h}_1$-regular subalgebras of EIV

References

[1] David W. Boyd. Reciprocal polynomials having small measure. Math. Comp., 35(152):1361–1377, 1980.

[2] Henri Cohen. A Course in Computational Algebraic Number Theory, volume 138 of Graduate Texts in Mathematics. Springer, Berlin, erste edition, 1993.

[3] Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. J. Symbolic Comput., 39(3-4):357–371, 2005.

[4] G. Ge. Algorithms related to multiplicative representations of algebraic numbers. PhD thesis, University of California, Berkeley, 1993.

[5] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. Math. Ann., 261(4):515–534, 1982.

[6] D.W. Masser. Linear relations in algebraic groups. In Alan Baker, editor, New Advances in transencendence theory, pages 248–262, New York, 1988. Cambridge University Press.

[7] Jean Michel Muller. Elementary functions: algorithms and implementation. Birkhäuser Boston Inc., Boston, MA, second edition, 2006.

[8] Arnold Schönhage. Equation solving in terms of computational complexity. In Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986), pages 131–153, Providence, RI, 1987. Amer. Math. Soc.

[9] Paul Voutier. An effective lower bound for the height of algebraic numbers. Acta Arith., 74(1):81–95, 1996.

[10] R. G. Ayoub and C. Ayoub. On the group ring of a finite abelian group. Bull. Austr. Math. Soc., 1:245–261, 1969.

[11] Jean-François Biasse and Claus Fieker. Improved techniques for computing the ideal class group and a system of fundamental units in number fields. Proceedings of ANTS 2012, to appear, 2012.

[12] A. Borel. Linear algebraic groups. Springer-Verlag, Berlin, Heidelberg, New York, second edition, 1991.

[13] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[14] C. W. Curtis and I. Reiner. Representation theory of finite groups and associative algebras. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962. Pure and Applied Mathematics, Vol. XI.

[15] W. Eberly. Decomposition of algebras over finite fields and number fields. Comput. Complexity, 1(2):183–210, 1991.

[16] W. Eberly. Decomposition of algebras over R and C. Computational Complexity, 1:211–234, 1991.

[17] W. Eberly and M. Giesbrecht. Efficient decomposition of associative algebras. In Y. N. Lakshman, editor, Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation: ISSAC'96, pages 170–178, New York, 1996. ACM.

[18] Willem A. de Graaf and Gábor Ivanyos. Finding splitting elements and maximal tori in matrix algebras. In Interactions between ring theory and representations of algebras (Murcia), volume 210 of Lecture Notes in Pure and Appl. Math., pages 95–105. Dekker, New York, 2000.

[19] Cornelius Greither. Improving Ramachandra's and Levesque's unit index. In Number theory (Ottawa, ON, 1996), volume 19 of CRM Proc. Lecture Notes, pages 111–120. Amer. Math. Soc., Providence, RI, 1999.

[20] Florian Hess, Sebastian Pauli, and Michael E. Pohst. Computing the multiplicative group of residue class rings. Math. Comp., 72(243):1531–1548, 2003.

[21] Graham Higman. The units of group-rings. Proc. London Math. Soc. (2), 46:231–248, 1940.

[22] Klaus Hoechsmann. Constructing units in commutative group rings. Manuscripta Math., 75(1):5–23, 1992.

[23] Klaus Hoechsmann. Unit bases in small cyclic group rings. In Methods in ring theory (Levico Terme, 1997), volume 198 of Lecture Notes in Pure and Appl. Math., pages 121–139. Dekker, New York, 1998.

[24] Jürgen Klüners and Sebastian Pauli. Computing residue class rings and Picard groups of orders. J. Algebra, 292(1):47–64, 2005.

[25] R. S. Pierce. Associative Algebras. Springer-Verlag, New York, Heidelberg, Berlin, 1982.

[26] M. Pohst and H. Zassenhaus. Algorithmic algebraic number theory, volume 30 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1989.

[27] Sudarshan K. Sehgal. Units in integral group rings, volume 69 of Pitman Monographs and Surveys in Pure and Applied Mathematics. Longman Scientific & Technical, Harlow, 1993. With an appendix by Al Weiss.

[28] C. C. Sims. Computation with Finitely Presented Groups. Cambridge University Press, Cambridge, 1994.

[29] Lawrence C. Washington. Introduction to cyclotomic fields, volume 83 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997.

[30] J. Adams, M. van Leeuwen, P. Trapa, and D. A. Vogan Jr. Unitary representations of real reductive groups. http://arxiv.org/abs/1212.2192, 2012.

[31] A. O. Barut and R. Rączka. Theory of Group Representations and Applications, World Scientific Publishing Company; 2nd rev. ed., 1986.

[32] N. Bourbaki. Groupes et Algèbres de Lie, Chapitres 4, 5 et 6. Hermann, Paris, 1968.

[33] R. W. Carter. Simple groups of Lie type, Pure and Applied Mathematics, vol. 28. John Wiley & Sons, London-New York-Sydney, 1972.

[34] F. du Cloux and M. van Leeuwen. Software for structure and representations of real reductive groups, v. 0.4.6, available from `http://www.liegroups.org`.

[35] A. M. Cohen, M. A. A. van Leeuwen, and B. Lisser. LiE a Package for Lie Group Computations, CAN, Amsterdam, 1992.

[36] H. Dietrich and W. A. de Graaf. A computational approach to the Kostant-Sekiguchi correspondence, accepted to be published in Pacific J. Math., 2012.

[37] The GAP Group, GAP – Groups, Algorithms, and Programming, v. 4.5.5. `www.gap-system.org`, 2012.

[38] V. V. Gorbatsevich, A. L. Onishchik and È. B. Vinberg. Lie groups and Lie algebras III. Springer, 1994.

[39] G. Ivanyos, L. Rònyai and W. A. de Graaf. Computing Cartan Subalgebras of Lie Algebras, Appl. Algebra in Eng. Comm. and Comp. **7**, 339-349, 1996.

[40] W. A. de Graaf. Lie Algebras: Theory and Algorithms. vol. 56 of North-Holl. Math. Lib. Elsevier Sci., 2000.

[41] S. Helgason. Differential Geometry, Lie Groups, and Symmetric Spaces. Academic Press, New York San Francisko London, 1978.

[42] J. E. Humphreys. Introduction to Lie algebras and representation theory. Second printing, revised. Graduate Texts in Mathematics, 9. Springer-Verlag, New York-Berlin, 1978

[43] G. Ivanyos, L. Ronyai, and J. Schicho. Splitting full matrix algebras over algebraic number fields, J. Algebra **354**, 211-223, 2012.

[44] V. G. Kac. Infinite dimensional Lie algebras. 3rd ed. Cambridge University Press, 1990.

[45] B. Kostant. On the conjugacy of real Cartan subalgebras. I. Proc. Nat. Acad. Sci. U.S.A. **41**, 967-970, 1955.

[46] A. W. Knapp. Lie groups beyond an introduction. 2nd ed. Progress in Math., 140. Birkhäuser, 2002.

[47] A. L. Onishchik. Lectures on Real Semisimple Lie Algebras and Their Representations. ESI Lectures in Mathematics and Physics. EMS, Zürich, 2004.

[48] J. Tits. Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples. Publ. Math. IHES **31**, 21-58, 1966.

[49] N. A. Vavilov. Can one see the signs of structure constants?, Algebra i Analiz, **19**:4, 34-68, 2007 (in Russian); St. Petersburg Math. J. **19**, 519-543, 2008 (English translation).

[50] J. F. Cornwell. Semi-simple real subalgebras of non-compact semi-simple real Lie algebras. I, II. Rep. Mathematical Phys., 2(4):239–261; ibid. 2 (1971), no. 4, 289–309, 1971.

[51] J. F. Cornwell. Semi-simple real subalgebras of non-compact semi-simple real Lie algebras. III. Rep. Mathematical Phys., 3(2):91–107, 1972.

[52] D. Cox, J. Little, and D. O'Shea. Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer Verlag, New York, Heidelberg, Berlin, 1992.

[53] Heiko Dietrich, Paolo Faccin, and Graaf. CoReLG, Computation with Real Lie Groups. A GAP4 package, 2013. in preparation, (http://science.unitn.it/~corelg/index.html).

[54] Heiko Dietrich, Paolo Faccin, and Willem A. de Graaf. Computing with real Lie algebras: real forms, Cartan decompositions, and Cartan subalgebras. J. Symbolic Comput., 56:27–45, 2013.

[55] Heiko Dietrich and Willem A. de Graaf. A computational approach to the kostant-sekiguchi correspondence. Pacific Journal of Mathematics, 265(2):349–379, 2013.

[56] E. B. Dynkin. Maximal subgroups of the classical groups. Trudy Moskov. Mat. Obšč., 1:39–166, 1952. English translation in: Amer. Math. Soc. Transl. (6), (1957), 245–378.

[57] E. B. Dynkin. Semisimple subalgebras of semisimple Lie algebras. Mat. Sbornik N.S., 30(72):349–462 (3 plates), 1952. English translation in: Amer. Math. Soc. Transl. (6), (1957), 111–244.

[58] Willem A. de Graaf. SLA - computing with Simple Lie Algebras. a GAP package, 2013. (http://science.unitn.it/~degraaf/sla.html), version 0.13.

[59] J. E. Humphreys. Introduction to Lie Algebras and Representation Theory. Springer Verlag, New York, Heidelberg, Berlin, 1972.

[60] A. W. Knapp. Lie groups beyond an introduction, volume 140 of Progress in Mathematics. Birkhäuser Boston Inc., Boston, MA, second edition, 2002.

[61] B. P. Komrakov. Maximal subalgebras of real Lie algebras and a problem of Sophus Lie. Dokl. Akad. Nauk SSSR, 311(3):528–532, 1990.

[62] A. N. Minchenko. Semisimple subalgebras of exceptional Lie algebras. Tr. Mosk. Mat. Obs., 67:256–293, 2006. English translation in: Trans. Moscow Math. Soc. 2006, 225–259.

[63] Arkady L. Onishchik. Lectures on Real Semisimple Lie Algebras and Their Representations. European Mathematical Society, Zürich, 2004.

[64] Atlas of Lie groups and representations. (http://www.liegroups.org).

[65] Jeffrey Adams and Fokko du Cloux. Algorithms for representation theory of real reductive groups. J. Inst. Math. Jussieu, 8(2):209–259, 2009.

[66] David H. Collingwood and William M. McGovern. Nilpotent orbits in semisimple Lie algebras. Van Nostrand Reinhold Mathematics Series. Van Nostrand Reinhold Co., New York, 1993.

[67] J. M. Ekins and J. F. Cornwell. Semi-simple real subalgebras of non-compact semi-simple real Lie algebras. IV. Rep. Mathematical Phys., 5(1):17–49, 1974.

[68] J. M. Ekins and J. F. Cornwell. Semi-simple real subalgebras of non-compact semi-simple real Lie algebras. V. Rep. Mathematical Phys., 7(2):167–203, 1975.

[69] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.5, 2012. (http://www.gap-system.org).

[70] Willem A. de Graaf. Constructing semisimple subalgebras of semisimple lie algebras. J. Algebra, 325(1):416–430, 2011.

[71] N. Jacobson. Lie Algebras. Dover, New York, 1979.

[72] M. Lorente and B. Gruber. Classification of semisimple subalgebras of simple Lie algebras. J. Mathematical Phys., 13:1639–1663, 1972.

[73] Mitsuo Sugiura. Conjugate classes of Cartan subalgebras in real semi-simple Lie algebras. J. Math. Soc. Japan, 11:374–434, 1959.

[74] Patrice Tauvel and Rupert W. T. Yu. Lie Algebras and Algebraic Groups. Springer-Verlag, Berlin Heidelberg New York, 2005.

[75] V. S. Varadarajan. Lie groups, Lie algebras, and their representations, volume 102 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1984. Reprint of the 1974 edition.